

مجلة

بحوث العلاقات العامة الشرق الأوسط



دورية علمية محكمة تصدر عن الجمعية المصرية للعلاقات العامة - العدد الثامن - يوليو/ سبتمبر ٢٠١٥

- دور وسائل التواصل الاجتماعي في تشكيل الوعي الاجتماعي في مواجهة الشعب والجريمة الرياضية من وجهة نظر الشباب الجامعي
أ.د/ ياس خضير البياتي (جامعة عجمان للعلوم والتكنولوجيا) ... ص ٩
- بين استراتيجية الاتصال واستراتيجية المؤسسة: أي رابط؟
د. رضا محمود المثاني (جامعة البحرين) ... ص ٥١
- أثر الدعاية الصهيونية على الرأي العام الفلسطيني خلال العدوان ٢٠١٤ على غزة - دراسة وصفية
د. زهير عبد اللطيف عابد عابد (جامعة الأقصى) ... ص ٧٥
- أنماط تعرض الجمهور السيناوي لشبكات التواصل الاجتماعي وعلاقته بتشكيل الرأي نحو الأحداث الجارية
د. إبراهيم حسن المرسي محمد (جامعة سيناء) ... ص ١٠٥
- ظاهرة الإعلام الجديد وتأثيرها على الأمن القومي
د. حمدي بشير محمد علي (جامعة القاهرة) ... ص ١٣٩
- مبادرات حماية حقوق الملكية الفكرية في البيئة الإلكترونية "حق المؤلف نموذجاً"
د. مها مصطفى عمر عبد العزيز (كلية الإمارات للعلوم والتكنولوجيا بأبو ظبي) ... ص ١٧٩
- صحافة المواطن: من متلقي إلى منتج المضامين الإعلامية
محمد أمين عبوب (جامعة حسيبة بن بو علي بالجزائر) ... ص ٢١٣

مستخلصات الرسائل العلمية:

- دور المواقع الإسلامية الافتراضية في تشكيل اتجاهات الشباب الجامعي العراقي نحو القضايا الدينية المعاصرة
"دراسة تحليلية ميدانية"
حردان هادي صايل ... ص ٢٣٣

(ISSN 2314-8721)

الشبكة القومية للمعلومات العلمية والتكنولوجية
(ENSTINET)

جميع الحقوق محفوظة ٢٠١٥ @ EPRA

www.cpra.org.eg

هيئة التحكيم العلمية للبحوث

أ.د علي السيد عجوة

أستاذ العلاقات العامة المتفرغ والعميد الأسبق لكلية الإعلام جامعة القاهرة

Prof. Dr. Thomas A. Bauer

Professor of Mass Communication at the University of Vienna

أ.د منى سعيد الحديدي

أستاذ الإذاعة والتلفزيون المتفرغ بكلية الإعلام - جامعة القاهرة

أ.د ياس خضير البياتي

أستاذ الإعلام بجامعة بغداد ووكيل عميد كلية المعلومات والإعلام والعلوم الإنسانية
جامعة عجمان للعلوم والتكنولوجيا

أ.د انشراح الشال

أستاذ الإعلام المتفرغ بكلية الإعلام جامعة القاهرة (دكتوراه الدولة فى الآداب والعلوم الإنسانية من فرنسا)

أ.د حسن عماد مكاوي

أستاذ الإذاعة والتلفزيون - عميد كلية الإعلام جامعة القاهرة

أ.د نسمة يونس

أستاذ الإذاعة والتلفزيون - كلية الإعلام جامعة القاهرة

أ.د محمد معوض إبراهيم

أستاذ الإعلام المتفرغ بجامعة عين شمس والعميد الأسبق لكلية الإعلام بجامعة سيناء

أ.د سامي السيد عبد العزيز

أستاذ العلاقات العامة والاتصالات التسويقية المتفرغ - العميد السابق لكلية الإعلام جامعة القاهرة

أ.د عبد الرحمن بن حمود العناد

أستاذ العلاقات العامة والإعلام بقسم الإعلام كلية الآداب - جامعة الملك سعود

أ.د محمود يوسف مصطفى عبده

أستاذ العلاقات العامة ووكيل كلية الإعلام لشئون خدمة المجتمع وتنمية البيئة - جامعة القاهرة

أ.د سامي عبد الرؤوف محمد طابع

أستاذ ورئيس قسم العلاقات العامة بكلية الإعلام - جامعة القاهرة

أ.د بسيوني إبراهيم حمادة

أستاذ الإعلام السياسي والرأي العام بكلية الإعلام - جامعة القاهرة
عميد شعبة الإعلام بالأكاديمية الدولية للهندسة وعلوم الإعلام ٦ أكتوبر

أ.د شريف درويش مصطفى اللبان

أستاذ الصحافة - كلية الإعلام جامعة القاهرة

أ.د حسن علي محمد علي

أستاذ الإذاعة والتلفزيون ورئيس قسم الإعلام بكلية الآداب - جامعة المنيا

أ.د عابدين الدردير الشريف

أستاذ الإعلام وعميد كلية الآداب والعلوم الإنسانية بجامعة الزيتونة - ليبيا

أ.د محمود حسن إسماعيل

أستاذ الإعلام وثقافة الأطفال - معهد الدراسات العليا للطفولة - جامعة عين شمس

أ.د حمدي حسن أبو العينين

أستاذ الإعلام وعميد كلية الإعلام والألسن - نائب رئيس جامعة مصر الدولية

أ.د عثمان بن محمد العربي

أستاذ العلاقات العامة والرئيس السابق لقسم الإعلام بكلية الآداب - جامعة الملك سعود

أ.د وليد فتح الله مصطفى بركات

أستاذ الإذاعة والتلفزيون - كلية الإعلام جامعة القاهرة

أ.د تحسين منصور رشيد منصور

أستاذ العلاقات العامة بكلية الإعلام جامعة اليرموك - الأردن

أ.د محمد عبد الستار البخاري

بروفيسور متفرغ بقسم العلاقات العامة والدعاية، كلية الصحافة، جامعة ميرزة أولوغ بيك القومية الأوزبكية

أ.د علي قسايسية

أستاذ دراسات الجمهور والتشريعات الإعلامية بكلية علوم الإعلام والاتصال - جامعة الجزائر ٣

أ.د رضوان بو جمعة

أستاذ الإعلام بقسم علوم الإعلام والاتصال - جامعة الجزائر



مجلة بحوث العلاقات العامة الشرق الأوسط

(JPRR.ME)

دورية علمية محكمة

العدد الثامن - يوليو / سبتمبر ٢٠١٥

مؤسسها

ورئيس مجلس الإدارة

د/ حاتم محمد عاطف

رئيس EPRA

رئيس التحرير

أ.د/ علي السيد عجوة

أستاذ العلاقات العامة المتفرغ والعميد
الأسبق لكلية الإعلام جامعة القاهرة
رئيس اللجنة العلمية بـ EPRA

مدير التحرير

أ.د / محمد معوض إبراهيم

أستاذ الإعلام بجامعة عين شمس
والعميد الأسبق لكلية الإعلام جامعة سيناء
رئيس اللجنة الاستشارية بـ EPRA

مساعدو التحرير

أ.د/ رزق سعد عبد المعطي

أستاذ العلاقات العامة بكلية الإعلام والألسن
جامعة مصر الدولية

أ.م.د/ الصادق راجح

أستاذ الإعلام المشارك
عميد الإعلام والعلاقات العامة بكلية الإمارات للتكنولوجيا
الإمارات العربية المتحدة

د/ السيد عبد الرحمن علي

مدرس العلاقات العامة بكلية الإعلام
جامعة سيناء

المراسلات

الجمعية المصرية للعلاقات العامة

جمهورية مصر العربية

الجيزة - الدقي

بين السرايات - ٢ شارع أحمد الزيات

Mobile: +201141514157

Tel : +2237620818

Www.epra.org.eg

Jpr@epra.org.eg

جميع حقوق الطبع والنشر محفوظة
للجمعية المصرية للعلاقات العامة

لا يجوز، دون الحصول على إذن خطي من الناشر، استخدام أي من المواد التي تتضمنها هذه المجلة، أو استنساخها أو نقلها، كلياً أو جزئياً، في أي شكل وبأي وسيلة، سواءً بطريقة إلكترونية أو آلية، بما في ذلك الاستنساخ الفوتوغرافي، أو التسجيل أو استخدام أي نظام من نظم تخزين المعلومات واسترجاعها، وتطبق جميع الشروط والأحكام والقوانين الدولية فيما يتعلق بانتهاك حقوق النشر والطبع للنسخة المطبوعة أو الإلكترونية.

الترقيم الدولي للنسخة المطبوعة
(ISSN 2314-8721)

الترقيم الدولي للنسخة الإلكترونية
(ISSN 2314-8723X)

ولتقديم طلب الحصول على هذا الإذن والمزيد من الاستفسارات، يرجى الاتصال برئيس مجلس إدارة الجمعية المصرية للعلاقات العامة على العنوان التالي:

EPRA Publications

Egyptian Public Relations Association, Giza, Egypt
Dokki, Ben Elsarayat -2 Ahmed Elzayat St.

بريد إلكتروني: chairman@epra.org.eg - jpr@epra.org.eg

موقع ويب: www.epra.org.eg

الهاتف : 818 - 02-376-20 (+2) - 151 - 14 - 15 - 0114 (+2) - 157 - 14 - 15 - 0114 (+2)

مجلة بحوث العلاقات العامة الشرق الأوسط

Journal of Public Relations Research Middle East

التعريف بالمجلة :

مجلة بحوث العلاقات العامة الشرق الأوسط دورية علمية تنشر أبحاثاً متخصصة في العلاقات العامة وعلوم الإعلام والاتصال، بعد أن تقوم بتحكيم هذه الأبحاث من قبل عدد من الأساتذة المتخصصين في نفس المجال، وهي تابعة للجمعية المصرية للعلاقات العامة أول جمعية علمية مصرية متخصصة في العلاقات العامة.

- المجلة معتمدة ولها ترقيم دولي ومصنفة دولياً لنسختها المطبوعة والإلكترونية من أكاديمية البحث العلمي والتكنولوجيا بالقاهرة، ومصنفة من لجنة الترتيبات العلمية تخصص الإعلام بالمجلس الأعلى للجامعات في مصر.
- المجلة فصلية تصدر كل ثلاثة أشهر خلال العام.
- تقبل المجلة نشر عروض الكتب والمؤتمرات وورش العمل والأحداث العلمية العربية والدولية.
- تقبل المجلة نشر إعلانات عن محركات بحث علمية أو دور نشر عربية أو أجنبية وفقاً لشروط خاصة يلتزم بها المعلن.
- يُقبل نشر البحوث الخاصة بالترقيات العلمية - وللباحثين المتقدمين لمناقشة رسائل الماجستير والدكتوراه.
- يُقبل نشر ملخصات الرسائل العلمية التي نوقشت، ويُقبل نشر عروض الكتب العلمية المتخصصة في العلاقات العامة والإعلام كذلك المقالات العلمية المتخصصة من أساتذة التخصص من أعضاء هيئة التدريس.

قواعد النشر:

- أن يكون البحث أصيلاً ولم يسبق نشره.
- تقبل البحوث باللغات: (العربية - الإنجليزية - الفرنسية) على أن يكتب ملخص باللغة الإنجليزية للبحث في حدود صفحة واحدة إذا كان مكتوب باللغة العربية.
- أن يكون البحث في إطار الموضوعات التي تهتم بها المجلة في العلاقات العامة والإعلام والاتصالات التسويقية المتكاملة.
- تخضع البحوث العلمية المقدمة للمجلة للتحكيم ما لم تكون البحوث قد تم تقييمها من قبل اللجان والمجالس العلمية بالجهات الأكاديمية المعترف بها أو كانت جزءاً من رسالة أكاديمية نوقشت وتم منح صاحبها الدرجة العلمية.
- يراعى اتباع الأسس العلمية الصحيحة في كتابة البحث العلمي ومراجعته ويراعى الكتابة ببنت (Simplified Arabic) (١٤) والعناوين الرئيسية والفرعية Bold.
- يتم رصد المراجع في نهاية البحث وفقاً للمنهجية العلمية بأسلوب متسلسل وفقاً للإشارة إلى المرجع في متن البحث وفقاً لطريقة APA الأمريكية.
- يقدم الباحث عدد (٢) نسخ مطبوعة من البحث ونسخة إلكترونية على CD مكتوبة بصيغة Word مصحوبة بسيرة ذاتية مختصره عنه.
- في حالة قبول البحث للنشر بالمجلة يتم إخطار الباحث بخطاب رسمي بقبول البحث للنشر. أما في حالة عدم قبول البحث للنشر فيتم إخطار الباحث بخطاب رسمي وإرسال جزء من رسوم نشر البحث له في أسرع وقت.
- إذا تطلب البحث إجراء تعديلاً بسيطاً فيلتزم الباحث بإعادة إرسال البحث معدلاً خلال أسبوع من استلام ملاحظات التعديل وإذا حدث تأخير منه فسيتم تأجيل نشر البحث للعدد التالي أما إذا كان التعديل جذرياً فيرسله الباحث بعد ١٥ يوم من إرسال الملاحظات له.

- قيمة نشر البحث ٨٥٠ جنيه مصري للمصريين من داخل مصر وللمصريين المقيمين بالخارج والأجانب ٤٥٠\$. .
- يتم رد مبلغ ٢٥٠ جنيهه للباحثين من داخل مصر ورد مبلغ ١٣٠ \$ للباحثين المصريين المقيمين بالخارج والأجانب في حالة رفض هيئة التحكيم البحث وإقرارهم بعدم صلاحيته للنشر بالمجلة.
- لا يزيد عدد صفحات البحث عن (٣٥) صفحة A4- في حالة الزيادة تحتسب الصفحة بـ ٢٠ جنيه مصري للمصريين داخل مصر وللمقيمين بالخارج والأجانب ٥\$. .
- يتم تقديم خصم خاص من قيمة النشر العلمى لعضوية زمالة الجمعية المصرية للعلاقات العامة من المصريين والجنسيات الأخرى بنسبة ١٠% ولأى عدد من المرات خلال العام.
- يُرسل للباحث عدد (٣) نسخة من المجلة بعد نشر بحثه، وعدد (٣) مستلة من البحث الخاص به.
- ملخص رسالة علمية (ماجستير) ٢٥٠ للمصريين ولغير المصريين ١٥٠\$. .
- ملخص رسالة علمية (الدكتوراه) ٣٥٠ جنيهه للمصريين ولغير المصريين ١٨٠\$. .
- على أن لا يزيد ملخص الرسالة عن ٨ صفحات. ويتم تقديم خصم ١٠% لمن يشترك في عضوية الجمعية المصرية للعلاقات العامة . ويتم إرسال عدد (٣) نسخ من المجلة بعد النشر للباحث على عنوانه بالبريد الدولى.
- نشر عرض كتاب للمصريين ٧٠٠ جنيهه ولغير المصريين ٣٠٠\$
- يتم إرسال عدد (٣) نسخ من المجلة بعد النشر لصاحب الكتاب على عنوانه بالبريد الدولى السريع.
- ويتم تقديم خصم ١٠% لمن يشترك في عضوية زمالة الجمعية المصرية للعلاقات العامة .
- بالنسبة لنشر عروض تنظيم ورش العمل والندوات من داخل مصر ٦٠٠ جنيهه ومن خارج مصر ٣٥٠\$. بدون حد أقصى لعدد الصفحات.
- بالنسبة لنشر عروض المؤتمرات الدولية من داخل مصر ٨٥٠ جنيهه ومن خارج مصر ٤٥٠\$ بدون حد أقصى لعدد الصفحات.
- جميع الآراء والنتائج البحثية تعبر عن أصحاب البحوث المقدمة وليس للجمعية المصرية للعلاقات العامة أى دخل بها.
- ترسل المشاركات باسم رئيس مجلس إدارة المجلة على عنوان الجمعية المصرية للعلاقات العامة- جمهورية مصر العربية - الجيزة - الدقى - بين السرايات - ٢ شارع أحمد الزيات، والإميل المعتمد من الجمعية jpr@epra.org.eg ، epra_cairo@yahoo.com أو إميل رئيس مجلس إدارة المجلة dr_hatematef2000@yahoo.com بعد تسديد قيمة النشر وإرسال صورة الإيصال التى تفيد ذلك.

الافتتاحية

في عامها الثالث تتواصل صدور أعداد المجلة بانتظام منذ بداية إصدارها في أكتوبر/ ديسمبر من العام ٢٠١٣ - ليصدر منها سبعة أعداد متتابعة تضم أبحاثاً ورؤى علمية متعددة لأساتذة ومتخصصين وباحثين من مختلف دول العالم.

والآن نقدم للباحثين في الدراسات الإعلامية والمهتمين بهذا المجال " العدد الثامن " من المجلة وهو يتضمن بحثاً ورؤى علمية للأساتذة والمساعدين والمدرسين وملخصات لرسائل علمية نُوقشت في أقسام وكليات الإعلام بالجامعات العربية المختلفة.

المجلة هي أول دورية علمية محكمة في بحوث العلاقات العامة بالوطن العربي والشرق الأوسط. وجد الأساتذة الراغبون في تقديم إنتاجهم للمجتمع العلمي بكافة مستوياته الفرصة للنشر على نطاق العالم العربي وبعض الدول الأجنبية التي تصل إليها المجلة من خلال مندوبيها في هذه الدول، وأيضاً من خلال موقعها الإلكتروني.

وباعتراف اللجنة العلمية (تخصص الإعلام) لترقية أعضاء هيئة التدريس إلى أساتذة وأساتذة مساعدين بالمجلة بعد أن اطلعت على العدد الأول وتم تقييمها بنفس درجة المجالات العلمية لأقسام الإعلام في الجامعات المصرية؛ أتاحت مجلة بحوث العلاقات العامة الشرق الأوسط الفرصة للنشر العلمي بها كنافذة جديدة لنشر بحوث طلبة وطالبات مرحلة الدكتوراه - ولبحوث أعضاء هيئة التدريس الراغبين في التقدم للترقي لدرجتي أستاذ مساعد وأستاذ.

ففي البداية نجد مشاركة لأحد كبار أساتذة الإعلام بالعالم العربي أ.د/ ياس خضير البياتي من (العراق) عن: " دور وسائل التواصل الاجتماعي في تشكيل الوعي الاجتماعي في مواجهة الشغب والجريمة الرياضية من وجهة نظر الشباب الجامعي".

كما يتضمن العدد بحثاً مقدماً للنشر العلمي بهدف تكوين رصيد للباحثين من أعضاء هيئة التدريس للتقدم للترقية لدرجة أستاذ منهم: د. رضا محمود المثاني من (تونس) والذي قدم دراسة بعنوان: " بين استراتيجية الاتصال واستراتيجية المؤسسة: أي رابط؟"، وقدم د. زهير عبد اللطيف عابد من (فلسطين) دراسة حول موضوع: " أثر الدعاية الصهيونية على الرأي العام الفلسطيني خلال العدوان ٢٠١٤ على غزة - دراسة وصفية".

أما د. إبراهيم حسن المرسي محمد من (مصر) شارك بدراسة في موضوع: " أنماط تعرض الجمهور السيناوي لشبكات التواصل الاجتماعي وعلاقته بتشكيل الرأي نحو الأحداث الجارية"، وشارك د. حمدي بشير محمد علي من (مصر) بدراسة حول: " ظاهرة الإعلام الجديد وتأثيرها على الأمن

القومي"، أما د. مها مصطفى عمر عبد العزيز من (السودان) فقدت ورقة علمية حول: " مبادرات حماية حقوق الملكية الفكرية في البيئة الإلكترونية (حق المؤلف نموذجاً) ".
ومن دولة (الجزائر) قدم محمد أمين عبوب ورقة علمية بعنوان: " صحافة المواطن: من متلقي إلى منتج المضامين الإعلامية ".

وللاستفادة من الرسائل العلمية تقدم الباحث حردان هادي صايل من دولة (العراق) لنشر ملخص دراسته للدكتوراه بعنوان: " دور المواقع الإسلامية الافتراضية في تشكيل اتجاهات الشباب الجامعي العراقي نحو القضايا الدينية المعاصرة - دراسة تحليلية ميدانية ".

وهكذا فإن المجلة ترحب بالنشر فيها لمختلف الأجيال العلمية من جميع الدول جيل الأساتذة وبحوثهم لا تخضع للتحكيم طبقاً للقواعد المتبعة للنشر العلمي في المجالات العلمية. أما البحوث المنشورة لأعضاء هيئة التدريس الراغبين في التقدم للترقية للدرجة الأعلى والطلاب المسجلين لدرجة الدكتوراه فتخضع جميعها للتحكيم من قبل الأساتذة المتخصصين.
وجميع هذه البحوث والأوراق العلمية تعبر عن أصحابها دون تدخل من هيئة تحرير المجلة التي تحدد المحكمين وتقدم ملاحظاتهم إلى أصحاب البحوث الخاضعة للتحكيم لمراجعة التعديلات العلمية قبل النشر.

ندعو الله أن يوفقنا لإثراء النشر العلمي في تخصص العلاقات العامة بشكل خاص والدراسات الإعلامية بشكل عام.

رئيس تحرير المجلة

أ.د/ علي عجوة

ظاهرة الإعلام الجديد وتأثيرها على الأمن القومي

إعداد

د/ حمدي بشير محمد علي(*)

(*) باحث في الشؤون السياسية العربية – كلية الاقتصاد والعلوم السياسية - جامعة القاهرة

ظاهرة الإعلام الجديد وتأثيرها على الأمن القومي

د/ حمدي بشير محمد علي
جامعة القاهرة

مقدمة:

تشهد المنطقة العربية في الوقت الراهن مع انتشار وتطور وسائل التواصل الاجتماعي تحديات أمنية في غاية الخطورة على كافة الأصعدة الاجتماعية والاقتصادية والسياسية، بشكل لم تعهده من قبل، إذ ازدادت معدلات الجريمة الإلكترونية واتسعت دوائرها، واستغل منفذوها وسائل الإعلام والاتصال الجماهيري الحديثة لتنفيذ مخططاتهم الإجرامية وتجنيب الشباب العربي، وإطلاق الحرب النفسية لتهريب الناس وزعزعة الأمن والاستقرار وصولاً لتنفيذ مآربهم المتطرفة وأهداف الجهات التي تقف خلفهم. ولهذا أصبحت ظاهرة الاعلام الجديد محط أنظار المراكز البحثية والدوائر الحكومية والمراكز الأمنية، لدراسة العوامل التي أثرت في تطورها، وآثارها على الاستقرار الاجتماعي والاقتصادي والسياسي والأمني، والتعرف على التحديات والتهديدات الأمنية التي تمثلها بالنسبة للاستقرار الوطني والقومي، وخاصة إذا كانت هذه الوسيلة تتيح التواصل عبر الحدود الوطنية واختراق المجال الوطني للدولة. وفي هذا الإطار تهتم هذه الدراسة بدراسة تأثير تكنولوجيا الإعلام الجديد على الأمن القومي ومجالاته السياسية والاقتصادية والاجتماعية والثقافية، وذلك من منظور استراتيجي أمني، والتعرف على الفرص والآفاق التي يتيحها الإعلام الجديد بالنسبة للأجهزة الأمنية ودوائر صنع القرار، بهدف الاستفادة من هذه التقنيات الجديدة في مواجهة تحدياتها بناء على التعرف على خصائصها وأطوار نموها وتداخلها مع الظواهر المختلفة، لأن التعرف على هذه الظاهرة وآثارها بلا شك يتيح للحكومات كيفية الاستفادة منها ووضع الحلول الملائمة لآثارها بناء على التشخيص العلمي السليم لها. ومع تنامي هذه التهديدات ، تحرص الدول على البحث عن أفضل الفرص المناسبة لضمان تحقيق الأمن، الذي يعتبر هو الهاجس الأول والأخير للدول والشعوب، وهو الركيزة الأساسية التي لا يمكن الاستغناء عنها أو التقليل من شأنها ، فانعدام الأمن يعنى انتشار الفوضى، ومن هنا فقد أصبح تحديد تأثير الاعلام الجديد على الأمن القومي مطلباً علمياً وتطبيقياً، وذلك لترشيد دور الاعلام لتدعيم الأمن الوطني لكل دولة بشكل يضمن حماية مصالحها في الداخل والخارج و يراعى الخصوصية الثقافية لها.

١ - مشكلة البحث:

تثير عملية التطور المستمر في تكنولوجيا المعلومات الهاجس الأمني لدى العديد من الدول، لأن تأثير هذه التقنيات الجديدة على أمن الدول في تزايد مستمر، وخاصة على المجالات العسكرية والأمنية، في التخطيط العسكري وإدارة الصراعات والحروب، وإدارة الأزمات الأمنية، ومن ثم تسعى هذه الدراسة إلى الإجابة على التساؤلات التالية :-

- أ- ما مدى تأثير تطور تكنولوجيا المعلومات واستخدام وسائل التواصل الاجتماعي في مفهوم الأمن القومي؟
- ب- هل يمثل الاعلام الجديد تهديداً للأمن القومي؟ وما هي أهم الآثار السلبية لتطور استخدام وسائل التواصل الاجتماعي على الأمن القومي؟
- ت- كيف يمكن الاستفادة من الإعلام الجديد في المجالات الأمنية والاستراتيجية؟
- ث- ما هي الاستراتيجية المثلى للتصدي للمخاطر والتهديدات الأمنية التي يفرضها هذا التطور؟.
- ج- ما هو مستقبل الأمن القومي في عصر تكنولوجيا المعلومات؟

٢ - أهمية البحث:

تكمن أهمية البحث في:-

- أ- أهمية دراسة الإعلام الإلكتروني عموماً بما يثيره من قضايا معاصرة تحظى باهتمام المراكز البحثية والأكاديمية، إذ أنشأت له الجامعات أقسام علمية في كليات الإعلام والمؤسسات الأمنية والشرطية والعسكرية.
- ب- أهمية دراسة الإعلام الجديد في إطار اهتمام الأجهزة الأمنية بمواجهة التصدي للجريمة الإلكترونية وتقادي حدوثها.
- ت- تزايد اهتمام الأجهزة الأمنية في العالم العربي بدراسة ظاهرة الاعلام الجديد وكيفية الاستفادة منها، فأنشأت العديد من الأجهزة الشرطية في العالم العربي بالفعل صفحات لها على الفيسبوك للتفاعل مع المواطنين، للرد على الشائعات وتصحيح المفاهيم الخاطئة لدى الجمهور بهدف تحقيق الاستقرار السياسي.
- ث- إدراك دوائر صنع القرار لأهمية دور هذه الوسائل الجديدة، لأن تزايد معدلات الجريمة الإلكترونية يفقد المواطنين الإيمان بسلطات الدولة ودورها في توفير بيئة آمنة.

٣ - منهج البحث:

تسعى الدراسة من خلال استخدام المنهج الوصفي و التحليلي إلى التعرف على تأثير تطور تكنولوجيا الإعلام الجديد في مفهوم الأمن القومي، وأهم الآثار والتهديدات الأمنية لتطور استخدام تكنولوجيا الإعلام الجديد في الصراعات الدولية والإقليمية والداخلية، والبحث في وضع استراتيجية مثلى للتصدي لهذه المخاطر والتهديدات الأمنية التي يفرضها هذا التطور، ومن ثم تنقسم هذه الدراسة إلى

ثلاثة مباحث رئيسية، يتناول الأول منها ظاهرة الإعلام الجديد وتأثيرها في مفهوم الأمن القومي، والثاني يتناول تأثير ظاهرة الاعلام الجديد على الأمن القومي، والثالث يتناول استراتيجية الأمن القومي في عصر تكنولوجيا المعلومات.

المبحث الأول

ظاهرة الإعلام الجديد وتأثيرها في مفهوم الأمن القومي

يهدف هذا المبحث إلى التعريف بظاهرة الإعلام الجديد، والعوامل التي أثرت في تطورها، وتأثيرها في مفهوم الأمن القومي ومجالاته، حيث تشهد مجتمعاتنا المعاصرة العديد من الظواهر الاجتماعية المتداخلة والمتراصة، نتيجة تأثير متغيرات هامة في حياتنا المعاصرة غيرت من مفهوم الأمن القومي، أهمها تطور استخدام وسائل الإعلام الاجتماعي، ولذلك من الأهمية بمكان أن نستعين بتحديد المفاهيم الأساسية، لاسيما الإعلام الجديد والأمن القومي، بهدف تشخيص الظاهرة وآثارها على الأمن القومي وأداء الأجهزة الأمنية، ولذلك يمكن تتبع تطور هذه ظاهرة وتأثيرها في مفهوم الأمن القومي من خلال مطلبين رئيسيين، يناقش المطلب الأول ظاهرة الاعلام الجديد ، ويتناول المطلب الثاني تأثيرها على مفهوم الأمن القومي، وذلك على النحو التالي :-

المطلب الأول

ظاهرة الإعلام الجديد

كان من أهم إنجازات ثورة تكنولوجيا المعلومات والاتصالات التي شهدتها العالم، والتطور المذهل لشبكة المعلومات الدولية (الإنترنت) وانتشار التقنيات الحديثة للاتصال، وتزايد تطبيقاتها في مجال الإعلام والاتصال، ظهور نوع جديد من الإعلام، وهو الإعلام الجديد، الذي يعتبر ظاهرة إعلامية جديدة فريدة من نوعها ، تتميز بسرعة الانتشار والوصول إلى أكبر عدد من الجمهور وبأقصر وقت ممكن وبأقل تكلفة، فبات يشكل نافذة مهمة جداً لنشر المعلومات والحصول عليها.

ولذلك تعتبر ظاهرة الإعلام الجديد ظاهرة اجتماعية وتقنية وثقافية فريدة من نوعها لا تزال تجذب انتباه الباحثين في مختلف التخصصات والمجالات الاجتماعية والثقافية والسياسية والأمنية ، بعد أن أمتد تأثيرها إلى الصعيد الإعلامي والثقافي والفكري والسياسي في مجتمعاتنا المعاصرة ، غير أن الطبيعة المعقدة للظاهرة وعدم تطورها بشكل كامل تضع تحدياً كبيراً أمام الباحثين للتنبؤ بمستقبلها، ولذلك يجد الباحثون في مختلف المجالات لدراسة تأثيرها ومحاولة صياغة استراتيجية متكاملة لمواجهة أخطارها والاستفادة منها.^١

وعلى الرغم من أنه لا يبدو أن هناك تعريفاً متفقاً عليه للإعلام الجديد حتى الآن، فمن الضروري أن نلقى نظرة سريعة على بعض أحدث التعريفات الهامة في المراكز الأكاديمية ، حيث تشير العديد من

التعريفات إلى أنه ظاهرة "تشمل مواقع الفيسبوك، تويتر، ماي سبيس وغيرها من وسائل الإعلام التفاعلية للتواصل الاجتماعي والسياسي والاقتصادي بين الأفراد والجماعات والحكومات".^٢

وقد عرف "أندرياس كابلان" و"مايكل هانلين" وسائل الإعلام الاجتماعية بأنها: "مجموعة من تطبيقات الإنترنت التي تبني على الأسس الأيديولوجية والتكنولوجية، والتي تسمح بإنشاء وتبادل المحتوى الذي يتم إنشاؤه، بينما التواصل الاجتماعي هو تضافر الناس وتفاعلهم مع بعضهم البعض، ويتضمن على المستوى الفردي العلاقات التي تربط الفرد بالآخرين في الدائرة الاجتماعية التي تشمل العائلة والأصدقاء، أو في الدوائر السياسية والاقتصادية الأوسع التي تتخطى الدوائر الاجتماعية للفرد إلى المجتمعات الأخرى".^٣

ويشير مصطلح الإعلام الجديد إلى ظهور نوع جديد من الإعلام، يحتوى على رسالة بمحتوى معين قد تكون نصية أو قد تكون صورة أو شريط فيديو، من خلال المرسل (المستخدم) إلى متلقي لها (مستخدم آخر)، ولكن الميزة التي أضافها أنه جعل بإمكان أى شخص أن يكون مرسلًا ومتلقيًا فى نفس الوقت، وأصبح بإمكان أى شخص أن يصبح محرراً أو معلقاً أو منتجاً أو مبدعاً لمحتوى معين، وبالتالي فقد أثر على هرمية الاتصال وتحول الإعلام من نمط الاتصال الرأسى إلى نمط جديد هو الاتصال الأفقى.^٤

وقد تعددت تصنيفات ومسميات هذه الظاهرة لدى المهتمين والمتخصصين فى مختلف المجالات ، الذي أطلقوا عليها : "الإعلام الجديد"، "الإعلام البديل"، "الإعلام الاجتماعي"، و "الاعلام الرقمية"... وغيرها من التعبيرات التي تعبر عن ظاهرة اجتماعية تقنية تشمل الشبكات الاجتماعية الافتراضية، والمدونات، والمنتديات الإلكترونية والمجموعات البريدية، وغيرها من الأشكال والأنواع المتعددة ، حيث يشير مسمى "الإعلام الاجتماعي إلى السمة والصبغة الاجتماعية التي تتسم بها مواقع التواصل فى ربط الأصدقاء والأقارب والزملاء فى العمل، أما مصطلح "الإعلام الجديد New Media" فهو مصطلح يميزه عن الإعلام التقليدى الذى يشمل وسائل الإعلام التقليدية مثل: الصحف والمجلات والإذاعة والتلفزيون..... الخ ، فهو يشير إلى حالة من التنوع فى الأشكال والتكنولوجيا والخصائص التي حملتها الوسائل الجديدة مقارنة بالتقليدية، بينما يشير مصطلح "الإعلام الرقمية Digital Media" إلى استخدام شبكة الإنترنت بالأساس فى نقل الأخبار وتبادل الآراء، و "الإعلام البديل" لأنه ظهر كبديل لوسائل الإعلام التقليدية فى تغطية الأحداث السياسية بسرعة ، وحققت ما عجزت عن تحقيقه الوسائل التقليدية، وقد أطلق البعض عليه أيضا مصطلح "العالم الافتراضي" الذى يرجع إلى هاوارد رينجولد الذى عرف المجتمع الافتراضي بأنه تجمعات اجتماعية تشكلت من أفراد فى أماكن متفرقة فى أنحاء العالم، يتقاربون ويتواصلون فيما بينهم عبر شاشات الكمبيوتر والبريد الإلكتروني، ويجمعهم اهتمام مشترك، وتحدث بينهم تفاعلات عن بعد من خلال آلية اتصالية هى الإنترنت.^٥

ويرى بعض المحللين أن هناك خلط بين التسميات التي ترتبط بوصف هذه الظاهرة مثل وصف العلاقات بين المستخدمين في الفيسبوك بـ "الأصدقاء"، أو "المعجبين"، أو "الأتباع"، فمصطلح "الأصدقاء" يمكن أن يكون مضللاً، لأن الاتصال بين شخصين لا يعنى بالضرورة الصداقة، ومن ناحية أخرى، هناك بعض المنصات مثل الفيسبوك، ماي سبيس، تستهدف مناطق جغرافية أو مجموعات لغوية معينة، على سبيل المثال، أطلقت في الولايات المتحدة الأمريكية واجهة باللغة الإنجليزية فقط، وصممت بعض الجماعات بعض المواقع العرقية والدينية، ومواقع لها توجه جنسي وسياسي، حتى مواقع للكلاب (Dogster)، ومواقع للقطة (Catster)، لذلك نجد أن هناك مجموعات تستخدم تلك المواقع لعزل نفسها حسب الجنس والعمر والمستوى التعليمي في بعض الأحيان.^٦

وعلى أية حال، إن ظاهرة الإعلام الجديد هي ظاهرة حديثة، وفي نفس الوقت يمكن أن ننظر إليها باعتبارها امتداداً لظاهرة أعم وأشمل وهي ظاهرة العولمة أو الكوكبة " Globalization، التي نتجت عن الثورة المعلوماتية والثورة التكنولوجية في تطور وسائل الاتصالات، بشكل أدى إلى تقليص المسافات وتحول العالم إلى ما يسمى بالقرية العالمية، وبالتالي فإذا كانت ظاهرة العولمة قد أثارت حولها العديد من الإشكاليات مثل "الخصوصية الثقافية" وإشكالية السيادة الوطنية.. الخ، فإن ظاهرة الإعلام الجديد تثير أيضاً حولها الكثير من الإشكاليات والتحديات المتعلقة بالمجالات السياسية والاقتصادية والأمنية.

إن النقطة الأهم في هذا الصدد، هي أن هذه الظاهرة لم تتطور بالصدفة إنما هي نتاج للعديد من العوامل، أهمها العوامل التكنولوجية والأيدولوجية والفكرية لدى مؤسسي المواقع الاجتماعية الذين كانوا حريصين على ابتكار وسائل جديدة للتواصل الاجتماعي، فقد أسس موقع الفيسبوك مارك زوكربرج وهو طالب في جامعة هارفارد الأمريكية، خوفاً من أن إدمانه للإنترنت قد يجعله يفقد أصدقائه بعد الانتهاء من الدراسة الجامعية، وإذا كانت الفرضية الأساسية للمجتمع الافتراضي منذ نشأته ترتكز على مشاركة الاهتمامات، التي تعد محدداً أيديولوجياً يستمد مرجعيته من الأطر الفكرية الحاكمة للمستخدمين، فإن الشبكات الاجتماعية تتميز بأمكانية الدخول والخروج إليها، وذلك تبعاً للتغيرات التي تطرأ على معتقدات وأفكار الفرد، بينما أغرت العوامل الاقتصادية مؤسسي وسائل التواصل الاجتماعي على تطويرها بعد تنافس الشركات العالمية على شراء تلك المواقع بمليارات الدولارات فتحول مؤسسيها من مبرمجين إلى مليارديرات بالصدفة، فأنتهت ثورة الاتصال الجديدة عدداً من المفاهيم كهرمية الاتصال، وأحادية مصدر الرسالة، كما استحدثت عدداً من المفاهيم الاتصالية الجديدة مثل: الوسائط الرقمية، والمجتمعات الافتراضية، والتشبيك الاجتماعي، وغيرها من المفاهيم والمصطلحات الأخرى، وتطورت سريعاً إلى وسيلة هامة للتأثير على المجتمع مع التطور السريع للإنترنت وتكنولوجيا الهاتف النقال والهاتف الذكي الحديث المجهز تجهيزاً جيداً بتطبيقات مختلفة تساعد على استخدام وسائل التواصل بفعالية.^٧

وعلى الرغم من تعدد تعريفات الإعلام الجديد إلا أنها تتفق في معظمها في أنه مصطلح يشير إلى استخدام كافة تقنيات الاتصال والمعلومات الرقمية في التواصل الرقمي، فجعل من الممكن نشر وتبادل المعلومات من خلال الأجهزة الإلكترونية المتصلة بالإنترنت، وهي خدمات يتم إنشاؤها وبرمجتها من قبل شركات كبرى لجمع أكبر عدد من المستخدمين لمشاركة الأنشطة والاهتمامات، وتوفر ميزات مثل المحادثة الفورية والتراسل العام والخاص ومشاركة الوسائط المتعددة من صوت وصورة وفيديو وملفات، فظهر ما يسمى بالمواطن الصحفي، فصار بإمكان الشخص الذي يعيش الأحداث أن يصورها أو يكتب عنها ويرسل ما يصور أو يكتب على الحائط الاجتماعي، دون أى حدود أو قيود على النشر، وبدون أى اعتبار لخطورة ما ينشر على أمن الدول، فتحوّلت هذه الوسائل من أداة للتسلية والتواصل الاجتماعي إلى أداة في أيدي وكالات الاستخبارات والتنظيمات الإجرامية والإرهابية وبشكل يهدد الأمن والسلم الوطنى بكل مجالاته الداخلية والخارجية، الفكرية والاجتماعية والاقتصادية والسياسية.

المطلب الثانى

أثر ظاهرة الإعلام الجديد فى مفهوم الأمن القومى

لقد تعرض العديد من المحللين لتأثير تكنولوجيا المعلومات فى مفهوم الأمن القومى، حيث يشمل مفهوم الأمن القومى كل أفعال الدولة التى تصدر عنها وتعكس وجهة نظرها لحماية أمنها، وتشمل الإجراءات التى تسعى إلى تحقيق أربعة أهداف مختلفة، وهى: سلامة وحماية المواطنين من أى اعتداء محتمل من قبل أى قوة داخلية أو خارجية، حماية الازدهار الاقتصادي ورفاهية مواطنيها، حماية القيم الوطنية الأساسية، وحماية القيم والتقاليد السائدة.^٨

وينبغى التذكير هنا بأن هناك عوامل كثيرة تؤثر على قدرة الدولة على تحقيق أهداف الأمن القومى، مثل الثروة، الجغرافيا، القدرات العسكرية، والبنية التحتية، القدرات الصناعية، والتعليمية، وهي في معظمها عوامل ملموسة، ويمكن قياسها بسهولة، وعوامل أخرى، مثل الاستراتيجية الوطنية، والقدرات التنظيمية والعلمية والفنية المعرفية، القدرات القيادية، والإرادة الوطنية والروح المعنوية، وهي عوامل غير ملموسة، وذاتية فى المقام الأول، وأقل قابلية للقياس بسهولة، والأهم من ذلك، يجب أن ندرك الأهمية النسبية لعوامل الأمن القومى لدولة ما، فالمعادلة ليست ثابتة، لأنها تتغير بمرور الوقت، وهذه حقيقة هامة ونحن نتحرك في عصر المعلومات، فمن المتوقع أن تنمو وتتغير عناصر القوة غير الملموسة والذاتية (مثل المعرفة) بأهمية أكبر من العلاقة التقليدية بين العوامل الملموسة، فبعض تهديدات الأمن القومى (على سبيل المثال، الغزو المسلح) قد أصبحت أقل احتمالاً من العوامل الأخرى (مثل التدهور الاقتصادي)، والأهم من ذلك أيضاً، أن الثورة التكنولوجية وتطور وسائل التواصل الاجتماعي وانتشارها قد غيرت بلا شك من طبيعة التهديدات الداخلية والخارجية، مثلما أدت التطورات التكنولوجية العسكرية

فى الماضى إلى تراجع أهمية عنصر الجغرافيا فى معادلة الأمن القومي للدول (مع ظهور حاملات الطائرات، والقاذفات النفاثة بعيدة المدى، والصواريخ العابرة للقارات) ^٩.

وكثيراً ما استخدم مفهوم "الأمن" كمرادف لمفهوم "الدفاع" فى الماضى، وهذا قد ارتبط ببعض الملابسات، لكن هناك اتفاق على أن الأمن هو مفهوم أكثر دقة و أكثر شمولاً من مفهوم الدفاع أو السياسة الدفاعية، فهو يشمل حماية الدولة، أراضيها، وشعبها من قبل القوات العسكرية من أى اعتداء من جانب أى قوة خارجية، ويشمل أيضاً حماية (ليس الضرورة بالوسائل العسكرية) موارد الدولة الاقتصادية والسياسية والاجتماعية والثقافية، الداخلية والخارجية، وغالباً ما تتضمن المكونات المحلية، القضايا الاقتصادية، مثل التجارة الخارجية والسياسة المالية، والسياسة النقدية، والعقوبات الاقتصادية، الأمن اللغوي، سياسة الهجرة، الدين، حقوق الإنسان، تطوير البنية التحتية، والعلاقة بين القدرات الاقتصادية و الأداء العسكري، قضايا التوظيف والرقابة الاستخباراتية، الإغاثة والكوارث، والعلاقات المدنية العسكرية، وفي الشؤون السياسية، يشمل قضايا الدبلوماسية، الاعتراف الدبلوماسي، تشكيل وحماية الأحلاف، وحماية "المصلحة الوطنية الحيوية"، فعند مستوى معين قد يتهدد الأمن القومي عندما تتهدد المصالح الوطنية الحيوية ^{١٠}.

على الرغم من اختلاف بعض الدول حول مصطلح "الأمن الوطنى" و "الأمن القومى"، حيث يرى البعض أن الأمن الوطنى يقصد به أمن دولة واحدة، أما الأمن القومى فهو أمن أكثر من دولة كمصطلح الأمن القومى العربى، ولكن فى الواقع أن التداخل والتكامل بين مستويات الأمن المختلفة (الوطنى والإقليمى والدولى) لا يجعل هناك تناقضاً بين هذه المستويات، لأنه لا تعارض بين الأمن المصرى أو السعودى أو العراقى أو أمن منطقة الخليج أو الأمن القومى العربى، لذلك فى رأى أن التسمية الأدق هى "الأمن القومى" ^{١١}.

ولقد أثرت التطورات التكنولوجية فى مفهوم الأمن القومى ومجالاته، فإلى جانب المجالات الاستراتيجية، المجال البرى والجوى والبحرى، أصبح لدينا مجالاً استراتيجياً جديداً تسعى معظم الدول الى أملاك كل أدوات التقدم التكنولوجى للسيطرة عليه، وفى هذا الفضاء الافتراضى تدور الكثير من الصراعات والحروب، لاسيما حرب المعلومات والتي هى عبارة عن مجموعة من الإجراءات (الهجومية) المتخذة لإفساد أو تدمير نظم معلومات العدو، أو الإجراءات (الدفاعية) التى تتخذ للحفاظ على سلامة نظام المعلومات الخاصة بكل دولة من الاستغلال والإتلاف، ويمكن تعريفها أيضاً " بأنها استخدام تكنولوجيا المعلومات للتأثير على إدراك العدو أو الجمهور المستهدف (الحرب النفسية)"، كما تعرف بأنها "جميع الإجراءات المتخذة للدفاع عن العمليات التى تستهدف المعلومات العسكرية، وتدمير نظم المعلومات وشبكات الاتصالات العسكرية، أو جميع الإجراءات التى تستخدم لتحديد أو استغلال قدرات العدو المادية والمعلوماتية والمعرفية، كحرب الهاكر، التى تهاجم الكمبيوتر وبرامجه، وحرب المعلومات الاقتصادية والتجسس الاقتصادي ^{١٢}، ومن ثم تضيف تكنولوجيا المعلومات ميزة استراتيجية

للقوى المتنافسة^{١٣}، وهو ما يدفع بالقوى المتنافسة إلى مهاجمة بعضها لاتلاف هذه الأصول وتغيير قيمتها.^{١٤}

وهذا يعنى أنه بلا شك، أثرت المتغيرات التكنولوجية الحديثة فى مفهوم " الأمن القومى " عموماً، وأحدثت تغييراً فى مجالات السيطرة والهيمنة الاستراتيجية، بل أن مجال الفضاء الإلكتروني هو فريد من نوعه يتأثر بالتغيرات التكنولوجية السريعة بدرجة أكبر من المجالات الأخرى، فجغرافيا الفضاء الإلكتروني هي أكثر قابلة للتغيير بكثير من البيئات الأخرى، فمن الصعب أن تتحرك الجبال والمحيطات ، ولكن يمكن أن تتحول أجزاء من الفضاء الإلكتروني بمجرد النقر على زر بالكمبيوتر، ومن ثم فقد انخفضت الحواجز أمام الإنترنت، باعتباره أداة أرخص وأسرع للتحرك فى جميع أنحاء العالم بدرجة أسرع وبأقل تكلفة من تكاليف تطوير حاملة طائرات، أو غواصات، ناهيك عن التهديدات الأمنية الداخلية الناتجة عن هذا التطور، حيث تتلشى الحواجز أمام الجماعات المارقة التى يمكن أن تلعب أدواراً هامة بتكاليف منخفضة نسبياً، وإذا كان لدى الحكومات احتكار واسع النطاق لاستخدام القوة فى العالم الحقيقى، ولديها معرفة وثيقة بالتضاريس، إلا أن هذه القدرات قد تتلشى فى العالم الافتراضى، حيث تنشط بعض الكيانات المجهولة فى بعض الأحيان، وتتضائل أمامها المسافة المكانية والزمنية.^{١٥}

وعلى هذا الأساس أشار بعض المحللين إلى أن هناك عدة أشكال متميزة من حرب المعلومات، وطالبوا بإرساء مفهوم أوسع، ويرون أنها تتطوي بطريقة أو بأخرى على " التلاعب والحرمان من المعلومات"، وقد خلصوا إلى إننا فى فجر عصر جديد سيخلق بيئة استراتيجية جديدة وإعادة تعريف لطبيعة الأمن القومي، وبالتالي الأهداف والغايات، والوسائل وطبيعة العمليات العسكرية. ولذلك أهتموا بتصنيف الصراع والحرب عبر شبكة الإنترنت وفقاً لأهدافه المحتملة إلى ثلاث فئات^{١٦}:

الفئة الأولى: وتشمل حرب المعلومات الشخصية، وهى هجوم ضد الخصوصية الفردية الإلكترونية وسجلات الفرد وملفاته الرقمية.

الفئة الثانية: وهى حرب المعلومات الاقتصادية، كالتجسس الصناعي، التجسس الاقتصادي.

الفئة الثالثة: وهى حرب المعلومات الدولية، كالحرب الإلكترونية، الإرهاب الإلكتروني، والتجسس الاستخباراتى، الحرب النفسية والتحريض على العنف.

أما البعض الآخر فقد صنف الصراع والحرب الإلكترونية إلى فئات أربع، وهى: حرب الشبكة، حرب القيادة والسيطرة، والحرب القائمة على المعلومات الاستخباراتية، والحرب النفسية من خلال عمليات الدعاية والتضليل الإعلامى للتأثير على سمعة الخصم، وما إلى ذلك من إجراءات تقع فى نطاق مفهوم "حرب المعلومات"، وقد يكون من المفيد هنا تقسيم الجهات الفاعلة فى الفضاء الإلكتروني إلى ثلاث فئات: حكومات ومنظمات وأفراد، حيث تشن الجهات الفاعلة الحرب الإلكترونية لتحقيق مجموعة متنوعة من الأهداف أهمها^{١٧} :-

أ- قهر الخصم وشل قدرته على الصد والاعتراض، والاستيلاء على الأراضي والموارد،

والإطاحة بالعدو.^{١٨}

ب- **الحصول على مزايا استراتيجية فى المجالات الأمنية والعسكرية**، وخاصة على صعيد وضع الاستراتيجيات العسكرية والأمنية والاستخباراتية، فمجال الفضاء الإلكتروني يختلف عن المجالات العسكرية التقليدية (البرى والبحرى والجوى)؛ فى تأثيره فى المجالات الثقافية والإعلامية، والإدراكية، فالاستراتيجية لا تستهدف فقط أهداف عسكرية، ولكن تستهدف أيضا المجتمعات (العرقية والدينية والثقافية أو المهنية) والبنى التحتية (شبكات الاتصالات السلكية واللاسلكية، و نظم والخدمات المصرفية، وما إلى ذلك).

ت- **الهجوم على البنية التحتية للاتصالات والشبكات** واختراق أجهزة الكمبيوتر أو الشبكات للدول (الخصوم) بهدف إلحاق الضرر باقتصادها أو بنيتها التحتية، والهجوم بالبرامج الخبيثة لتعطيل الأنظمة أو سرقة الممتلكات الفكرية كوسيلة لزيادة قدرات الخصم من الموارد الاقتصادية، أو إلحاق الخسائر الاقتصادية بالخصم باستهداف الأنظمة الإلكترونية فى المرافق العامة والصناعات ومحطات الطاقة الكهربائية والنوية التى يتم التحكم فيها بواسطة أجهزة الكمبيوتر.^{١٩}

ث- **جمع المعلومات أو اتلافها أو نشر المعلومات الخاطئة والمغلوطة بهدف الاضرار بالخصوم ومصالحهم**، أو لإحداث التوازن والتكافؤ بين طرفى الصراع، ويتحقق ذلك باستغلال الثغرات الأمنية فى أنظمة وبرامج الكمبيوتر لاختراق جدار الحماية، والتسلل التام لإتلاف البيانات، أو سرقة المعلومات، أو الرصد (جمع المعلومات الاستخباراتية)، أو نشر الرسائل الكاذبة، ونشر الأفكار والأيدولوجيات السياسية، والوصول إلى البيانات لغرض الابتزاز، أو إرسال الفيروسات (برنامج مصمم لتدمير النظام عن بُعد مثل حصان طروادة وهو برنامج يهدف إلى إضعاف القدرات الدفاعية من الداخل، وبرامج أخرى لجمع كلمات السر والكشف عن المعلومات)^{٢٠}، ونشر المعلومات للإقناع وجذب الاهتمام حول بعض القضايا.

ولكن يجب ملاحظة أن تحقيق هذه الأهداف يتوقف على الاعتبارات التالية^{٢١}:

أ- الهجوم الإلكتروني هو اختراق أمنى لتعطيل الأنظمة الإلكترونية، وتلجأ إليه الجماعات والدول سواء لأغراض أيديولوجية أو جنائية، وقد يكون لدى الجماعات قدرات كبيرة من نظم الاتصالات لشن الهجمات المتطورة.

ب- يمكن أن يلحق القرصنة ضرراً كبيراً بالحكومات الكبيرة عبر شبكة الإنترنت، ولكن هذا لا يجعلهم فى مستوى متكافئ فى المجال الإلكتروني، فليسوا بنفس القدرات^{٢٢}.

ت- تتطور عملية الهجوم عبر عدة مراحل، حيث يبدأ المهاجم بجمع المعلومات حول الهيكل التنظيمي لهذا الهدف، ويحدد الأشخاص الذين يشغلون المناصب العليا للوصول لمعلومات حساسة، عادة ما يتم إنجاز جمع المعلومات الشخصية عن طريق الحصول على المعلومات

العامة والشخصية على الشبكات الاجتماعية، وبمجرد أن يتم تحديد اللاعبين الرئيسيين يجري بذل الجهود لسرقة وثائق أجهزة الكمبيوتر الخاصة بهم، بإدراج أداة الوصول عن بعد بواسطة البريد الإلكتروني المرسل من مصدر موثوق به مع محتوى ذو صلة، وبالتالي ينصح بفلترة البريد المزعج، لان فتح البريد يسمح بإدراج حضان طروادة داخل شبكة الشركة، وبالتالي سرقة الموارد الداخلية.^{٢٣}

ث- الحرب الالكترونية ترتبط بحالة صراع داخلي أو دولي أو اقليمي، اجتماعي أو اقتصادي أو سياسي، هي سلاح غالباً ما يفضله الطرف الضعيف ضد القوي، لأنها تتميز بتكلفة منخفضة نسبياً، وأن الدول المتقدمة والدول الغنية بمواردها وقدراتها الاقتصادية والعسكرية هي الأكثر عرضة للهجمات عبر شبكة المعلومات لأنهم أكثر اعتماداً على تلك الأنظمة من الدول الفقيرة والمتخلفة.

ج- فشل الهجوم عبر الإنترنت من قبل الطرف الأضعف على الطرف الأقوى، يعرض الطرف الأضعف للانتقام، وفي مثل هذه الحالة، فإن الطرف الأقوى سوف يكون أكثر قوة، وأكثر فتكاً، ولديه كل الخيارات للرد.

ح- الطرف الأضعف قد يكون قادر على التسبب في بعض الإزعاج للطرف الأقوى من خلال الهجوم عبر الانترنت، ولكن عندما يسعى لإجباره وإرغامه من خلال الحرب الالكترونية، فإنه يتعرض لخطر حقيقي ومدمر جداً بسبب الرد الانتقامي المحتمل من جانب الطرف الأقوى.

خ- الرد لا يقتصر على عالم الإنترنت؛ فقد يرد الطرف الأقوى بكل ما في وسعه، وعلى هذا الأساس فمعركة الإرادة الفولاذية قد تقوى من عزيمة العدو وتشد مقاومته، ولكنها تتحطم في أقرب وقت.

د- الحرب الإلكترونية ليست أداة حاسمة لتحقيق النصر أو الهزيمة في صراعات المستقبل فهي تبدو كأسلوب يستهدف إثارة غضب الثور الجريح، ومع ذلك، فمن الأرجح أن تلعب دوراً متزايداً كأداة تمكينية في حروب المستقبل، والأكثر احتمالاً أن تكون أداة تمارس من جانب الطرف الضعيف ضد الطرف القوي.

وعلى أية حال فاننا نخلص من هذا المبحث بنتيجة مفادها أن تكنولوجيا الإنترنت والإعلام الجديد قد أثرت في مفهوم الأمن القومي ومجالاته وفي اتساع نطاق الحرب بين الدول بل واتساع نطاق الجريمة المنظمة بشكل يتطلب ضرورة إعادة النظر في التعامل مع مثل هذه المتغيرات الجديدة.

المبحث الثاني

الإعلام الجديد وتأثيره على الأمن القومي

يتناول هذا القسم من الدراسة أهم التهديدات التي يمثلها الإعلام الجديد للأمن القومي ومصالح الدول في الداخل والخارج، وبصفة خاصة تأثيره في المجال السياسي والاقتصادي العسكري والأمني، ومن ثم فهو يفرض العديد من المخاطر بالنسبة للجيش والشرطة، ولذلك يهتم هذا القسم بدراسة وتحليل استخدام الانترنت وتكنولوجيا الإعلام الجديد في الحروب والتجسس والغزو الثقافي والاقتصادي ونشر الأفكار الايدلوجية، وكذلك استخدام الجماعات الإرهابية للهجوم على المنشآت الحكومية وتهديد مصالح الدول، بلاشك إن التكلفة الاقتصادية والأضرار المادية الناتجة عن هجمات الانترنت سواء كانت من جانب الدول أو الجماعات، وسواء كان مصدرها من داخل الدولة أو خارجها، هي بالتأكيد باهظة وفي تزايد مستمر مع استمرار هذه الهجمات.

المطلب الأول

أثر الإعلام الجديد على الأمن القومي

يمكن تصنيف التهديدات التي يمثلها الإعلام الجديد من حيث المجالات التي يستهدفها وتهديد مصالح الدول في الداخل والخارج، فعلى المستوى الداخلي، يمكن أن يستهدف الخصوم الأمن الفكري والاقتصادي والاجتماعي والسياسي، موارد الدولة الاقتصادية والبشرية، نشر الشائعات والدعاية الكاذبة والفتن الطائفية، سرقة الحماية الفكرية، تهديد العلامات التجارية للشركات واستقرار الأسواق والأسعار، تحريك المظاهرات والإضرار بعلاقة الدولة بمواطنيها وعلاقة الجماعات والأحزاب بعضها ببعض، ما يهدد سلطان الدولة وسيادتها على أراضيها وقدرتها على فرضها نظامها القانوني وحماية نظامها الاجتماعي، وعلى صعيد الأمن الخارجي، يؤدي استخدام الإعلام الجديد لأغراض التجسس الإلكتروني والحرب النفسية والإرهاب إلى الإضرار بمصالح الدولة وأمنها القومي^{٢٤}، ولذلك يمكن تحليل هذه الظواهر وتأثيرها على المصالح السياسية والأمنية على النحو التالي:

أولاً: تهديد الأمن الاقتصادي:

الأمن الاقتصادي هو حماية مصالح الدولة الاقتصادية في الداخل والخارج، كحماية منشآتها الاقتصادية وقطاعاتها الانتاجية، ومراقفها العامة، وكذلك المؤسسات المالية البنوك والشركات والأفراد، لذلك يمثل الانترنت وتكنولوجيا الإعلام الجديد تهديداً للأمن الاقتصادي للدول، بسبب الهجمات الالكترونية التي تستهدف المؤسسات الاقتصادية والمالية العامة والخاصة، بهدف سرقة البيانات أو غسل الأموال أو نقل الأموال، أو نشر الشائعات الاقتصادية حول أسعار بعض السلع الاستراتيجية، أو بالهجوم الإلكتروني المباشر لتعطيل أنظمة شبكات الاتصال والإنترنت في المنشآت النفطية للتأثير على ضخ البترول وعرض البترول ومن ثم مستويات الأسعار في الأسواق الدولية، كذلك الهجوم على شركات الطيران للتأثير على حركة الطيران والسياحة بين الدول، والهجوم الإلكتروني على البنوك والهجوم على

البورصة بهدف التأثير على حركة أسعار الأسهم، أو الهجوم على منشآت الطاقة بهدف تعطيلها وتخریبها وتكبيد الدولة خسائر اقتصادية، بالإضافة إلى التحديات التي تواجهها الشركات والمؤسسات الخاصة مثل سرقة العلامات التجارية وتزويرها، والاحتيال الاعتداء على حقوق الملكية الفكرية المتعلقة بعمليات الإنتاج والتصنيع، وهو الأمر الذي يمثل تهديداً أمنياً لمصالح الدولة ومرافقها العامة وممتلكات الأشخاص والشركات، ومن ثم يفرض تحدياً كبيراً على قدرة الدولة على حماية الممتلكات العامة والخاصة.

وفي الواقع، إن تقدير التكلفة الاقتصادية والخسائر التي يمكن أن تنتج عن القرصنة هي بالتأكيد تكفة باهظة، ولكن السؤال الهام هنا، هو هل نحن نستطيع بالفعل تقدير القيمة المالية للوصول إلى المعلومات بكل دقة؟ هل يمكن تقدير القيمة الحقيقية للمعلومات المسروقة، عندما يتعلق الأمر بسرقة الملكية الفكرية مثلاً، فلا تزال الدراسات تواجه بعض المشكلات المتعلقة بعدم وجود بيانات كافية، حيث يستخدم الباحثون أساليب إحصائية لاشتقاق التقييمات من بيانات جزئية، وهناك صعوبة في تقدير حجم الضرر، وحتى الآن يبدو أن التقديرات النقدية بواسطة الأساليب الإحصائية غير كافية على أساس عدم كفاية البيانات أو المبالغة في تقديرها، لعدم مصداقية مصادر المعلومات وعدم ملائمة الأسلوب الإحصائي لهذا النوع من الأبحاث.^{٢٥}

ولا تزال بعض الأسئلة الهامة لفهم الظاهرة تحتاج إلى إجابة، وترتبط هذه الأسئلة بالقيمة النقدية للمعلومات وتقييم القيمة السوقية لها في الحاضر أو المستقبل، وبلا شك إن تقديم صورة أقل مصداقية بتضخيم الضرر من شأنه أن يؤدي إلى رد فعل معاكس، وبالتالي إن مناقشة التقديرات النقدية للضرر الناتج عن الجرائم الإلكترونية يحتاج إلى دراسة متأنية ومتخصصة.^{٢٦}

وعلى الرغم من المبالغة في بعض التقييمات النقدية، بسبب عدم وجود اتفاق على الأضرار المباشرة وغير المباشرة الناجمة عن جرائم الإنترنت، لكن لا خلاف على تزايد الضحايا المحتملين من المواطنين والجماعات، وتشير التقديرات إلى خسائر بمليارات الدولارات لحقت ببعض الحكومات نتيجة أعمال القرصنة، وتشير بعض التقديرات إلى أن خسائر شركة أنتل وحدها نتيجة سرقة البيانات قد بلغت أكثر من تريليون دولار في عام ٢٠٠٨.^{٢٧}

وعلى أية حال يمكن تلخيص مظاهر تأثير الإعلام الجديد على الأمن الاقتصادي للدول فيما يلي :

أ- استهداف المرافق العامة والمنشآت الحيوية^{٢٨}:

- يتزايد قلق أجهزة الأمن القومي من قيام بعض العناصر الاجرامية والارهابية من استهداف المرافق العامة، لا سيما محطات الطاقة الكهربائية ومحطات المياه والصرف الصحي والطاقة النووية، حيث تم الكشف عن العديد من عمليات الاقحام لمحطات الطاقة النووية والصرف الصحي في العديد من الدول (مثل شركات إكسون موبيل، ماراتون أويل وكونوكو فيليبس، التي استهدفت في عام ٢٠٠٨).^{٢٩}

- تتعرض صناعات النفط والغاز لنقاط ضعف مماثلة، من خلال سرقة معلومات المديرين التنفيذيين عن التتقيب والاكتشاف، وقد تشمل استخدام برامج التجسس، حيث أن هذه الشركات تتفق مئات الملايين على استكشاف الطاقة، ويقوم المهاجم بكسب ميزة مالية هائلة من خلال نقاط الضعف الهيكلية.

- أصبحت الشركات الصغيرة والمتوسطة الحجم، أهدافاً متزايدة للقصد الجنائي، ويمكن لمجرمي الإنترنت بسهولة الحصول على الميزانيات العمومية للشركات؛ والوصول إلى البيانات المالية وميزانيات الشركات الخاصة، وسرقة طريقة إنتاج المنتج، أو سرقة خارطة أعمال البحث والتطوير للخطة الصناعية وسرقة الملكية الفكرية؛ أو سرقة أرقام بطاقات الائتمان.

ب- نشر الشائعات الاقتصادية ٣٠:

- يساهم انتشار الشائعة في الترويج لسلع تجارية لا تساوى في قيمتها الحقيقية قيمتها الشرائية، وقد يؤدي انتشار الشائعات في الحد من انتشار سلع تجارية خالية من أي عطب أو عيب تجاري، ومع ذلك فإن انتشار الشائعات حولها يمكن أن يكون سبباً لخسارات كبيرة ، ويمكن لانتشار شائعة أن يسهم في الترويج لسلع اقتصادية عديدة لا تتوفر فيها حتى الحدود الدنيا من المواصفات المطلوبة، كما إن إطلاق الشائعة الكاذبة عن التردى الاقتصادي وخسائر البورصة يؤثر بلا شك على اقتصاد الدولة، وبالتالي فيمكن أن تخلق الشائعة أزمة اقتصادية.^{٣١}

ج- الاعتداء على حقوق الملكية الفكرية ٣٢:

- يؤدي استخدام مواقع التواصل الاجتماعي إلى إثارة الكثير من المسائل القانونية المتعلقة بالملكية الفكرية، فسهولة نشر المحتوى وتوزيعه في مواقع التواصل الاجتماعي يجعل من السهل مخالفة قوانين حقوق الملكية الفكرية للسطو على الحقوق الفكرية للغير بقصد أو بدون قصد.

- تجاوزت التكلفة العالمية من هجمات قرصنة الكمبيوتر حول الملكية الفكرية وحدها تريليون دولار في عام ٢٠٠٩ بسبب سرقة معلومات شخصية، والاحتيال عبر الإنترنت، وسرقة الهوية الرقمية، والتعدى على الخصوصية.^{٣٣}

والواقع الفعلي يشير الى حالات وشواهد ووقائع متكررة لظاهرة الهجوم الإلكتروني على المنشآت والمرافق العامة في بعض الدول، نسوق منها على سبيل المثال لا الحصر، بعض الحالات التي وقعت مؤخراً وأهمها:

أ- الهجوم الإلكتروني على موقع الخطوط الجوية البولندية في مايو ٢٠١٥ ما أسفر عن الغاء ١٠ رحلات جوية، وحجز ١٤٠٠ مسافراً في المطار لعدة ساعات.

ب- الهجوم الإلكتروني لكوريا الشمالية على شركة سونى بيكتشرز في عام ٢٠١٤، مما أسفر عن إلغاء الشركة عرض فيلم "المقابلة" الساخرة الذي يدور حول مؤامرة وهمية لووكالة الاستخبارات الأمريكية لاغتيال الزعيم الكورى كيم جونج - أون.

- ت- الهجوم الإلكتروني على شركات الطيران والبورصة الإسرائيلية وتعطيلهما مؤقتاً عام ٢٠١٤.
- ث- الهجوم الإلكتروني لكوريا الشمالية على شبكات المؤسسات المالية ومحطة البث الإذاعي الكورية YTN في كوريا الجنوبية في مارس ٢٠١٣.
- ج- الهجوم الإلكتروني على شركة ارامكو السعودية في عام ٢٠١٥ بهدف وقف ضخ الزيت والغاز محلياً وعالمياً.

ثانياً: تهديد الأمن السياسي :

يهتم الأمن السياسي بحماية مصالح الدولة السياسية وسيادتها الوطنية على كامل إقليمها الوطني واستقرارها السياسي والمحافظة على وحدة الدولة الوطنية واندماجها الوطني واستقرار العلاقة بين الجماعات والطوائف المختلفة، وحماية حدودها ووحدة أراضيها وسلامتها من أي تهديد داخلي أو خارجي، ولذلك فإن استخدام الإنترنت ووسائل الإعلام الجديد في الإضرار بالأمن السياسي للدولة، وهناك الكثير من الممارسات السلبية كنشر الشائعات وانتهاك القانون الوطني ونشر الفتن الطائفية بين أبناء المجتمع بهدف إحداث حالة من الانقسام المجتمعي أو الاستقطاب السياسي بشكل يؤدي إلى المواجهات الطائفية والجمود السياسي والمؤسسي في مؤسسات الدولة، وفي هذا الصدد يمكن الإشارة إلى بعض الحالات والشواهد والوقائع المتكررة لظاهرة الهجوم الإلكتروني على مصالح الدول وأمنها السياسي، وأهمها:-

- أ- الهجوم الإلكتروني على موقع البرلمان الألماني في مايو ٢٠١٥، ما أسفر عن إتلاف النظام المعلوماتي، وهو الأمر الذي يكبد الدولة ملايين من اليورو لتغيير انظمة الكمبيوتر.
- ب- الهجوم الإلكتروني على موقع وزارة الخارجية السعودية مايو ٢٠١٥، ما أسفر عن تسريب ونشر ويكيليكس لحوالي ٧٠ ألف وثيقة من بين ٥٠٠ ألف وثيقة.
- ت- هجمات متكررة من جانب كوريا الشمالية على شركة سوني بيكتشرز بهدف التشويش على الحملة التي تقودها الولايات المتحدة ضد البرنامج النووي لكوريا الشمالية.^{٣٤}
- ث- الهجوم الإلكتروني المتكرر على مواقع الخارجية الأمريكية والبيت الأبيض ووزارة الدفاع بهدف اختراق النظم الأمنية والمعلوماتية في المؤسسات الحكومية الأمريكية.
- ج- الهجوم الإلكتروني على المستشفيات وتهديد حياة المرضى عن طريق الوصول الى مضخات العقاقير وتعديل الجرعة وهو ما يترتب عليها وفاة المريض.

ويمكن تلخيص مظاهر تهديد الأمن السياسي للدول فيما يلي:

- أ- تهديد سيادة الدولة وسلطانها في فرض النظام القانوني:^{٣٥}
- ضعف قدرة الدولة على القيام بوظائفها: لم تعد الدولة قادرة على السيطرة على قطاعات هامة اعتادت السيطرة عليها لعهود طويلة.^{٣٦}
- انتهاك القوانين الوطنية: سرعة الوصول إلى الفضاء الإلكتروني في جميع أنحاء العالم يتحدى

بالتأكيد المفاهيم التقليدية للسيادة الوطنية، الأمر يزيد أكثر من صعوبة التحقيق والمقاضاة في الجريمة الإلكترونية في ظل عدم وجود تشريعات وقوانين أو اتفاقيات لمنع الجريمة الإلكترونية بين الدول.

- **اختراق حدود الدول** : لم تعد الدولة قادرة على منع الممارسات الضارة من اختراق أراضيها، اختراق الإنترنت ووسائل التواصل الاجتماعي للحواجز والحدود الدولية يؤثر في قدرة الدولة على منع الجريمة الإلكترونية عبر حدودها.

- لم تعد الحكومات هي الجهات الفاعلة الوحيدة التي يمكنها شن الهجمات الإلكترونية الكبيرة، فلا تزال الجماعات الإرهابية مهتمة بالوصول إلى قدرات الإنترنت لتمويل أنشطتها وتنفيذ عملياتها.

- الغزو الفكري والثقافي على المجتمعات العربية، بالترويج لمضامين وتقاليد خارجة على الثقافة العربية والإسلامية بعد أن تحولت إلى قنوات تجارية توظف إطاراً للتنافس والتريح التجاري، واستهداف القيم الأخلاقية والعقائدية.

ب- التأثير على الرأي العام^{٣٧}:

- **تعبئة التمرد وحشد رأي عام مناهض**: تؤدي الشائعات عبر وسائل الإعلام الجديد خلال فترات الأزمات مثل الأزمات الاقتصادية والنزاعات المسلحة والكوارث الطبيعية إلى تدهور الموقف السياسي، وانتشار رأي عام مناهض من جانب السكان المتضررين، ويمكن أن تؤدي إلى ظهور أفكار بديلة، وأحياناً تخريبية تمثل تهديداً كبيراً للمصالح السياسية، ويمكن أن يتفاقم الوضع بظهور حركات التمرد، التي تطالب بتخصيص الموارد اللازمة، ويمكن أن توفر وسائل الإعلام الجديد وسيلة لبناء قاعدة متضامنة من المتمردين، وتسهل عملية التعبئة السياسية للمتمرد.

- تظهر ضمن تشكيلة التفاعلات الافتراضية تفاعلات تمردية ، وذلك لأن الفرد يستطيع أن يقول ما يريد خارج الضوابط التقليدية للمجتمعات، فالمجال مفتوح في الفضاء الرقمي للاتفاق علي التظاهرات من دون قيود المكان، ومن ثم فإن المخاطر والتحديات السياسية تكمن في تحول تلك المظاهرات أو الإضرابات إلى حركات تمرد علي المستويات القومية أو العالمية، حيث تكون تجمعاتها الافتراضية آلية رئيسية تساهم في الاتفاق علي مناهضة الحكومات^{٣٨}.

- **الانقسام السياسي**: ويمكن أن تخلق الشائعات أزمة سياسية أيضاً، عندما يشاع أن هناك جبهة سياسية معينة تشكك في نوايا حزب آخر وأنه مثلاً يريد الاستحواذ على الحكم، وفي أوقات الحروب قد تصل الشائعات إلى ما لا تستطيع الأسلحة الحربية الوصول إليه في محاولة للتأثير في طريقة أداء الأطراف المشاركة في ميدان القتال، والتأثير على إرادة القتال لدى الطرف الآخر.^{٣٩}

- **إثارة الصراع السياسي**: عند حدوث الشغب يؤدي ترويج الشائعات عبر وسائل التواصل الاجتماعي إلى التأثير على معنويات الشعب، وقد تجد قوى سياسية واجتماعية متنوعة في

استخدام الشائعات بما يحقق لها مواقع نفوذ وسلطة على حساب مواقع سياسية أخرى، وتستخدم الشائعات في كثير من الأحيان في الصراعات السياسية المختلفة، فتسهم في تغيير موازين القوى وإثارة الصراع السياسي.^{٤٠}

- **تعبئة الحركات الانفصالية:** يمكن أن تتطور حركات التمرد إلى ظهور حركات انفصالية تهدد تكامل وحدة إقليم الدول وسيادتها على أراضيها، وخاصة في الدول العربية، حيث هناك العديد من الجماعات والأقليات التي تتطلع إلى الانفصال عن الدولة الأم، وربما تستخدم هذه الأدوات الجديدة في تحقيق ذلك.

- **المواجهات الطائفية:** قد تستخدم بعض الجماعات الدينية المتطرفة وسائل الإعلام الجديدة لتحريض على المواجهات الطائفية والدينية، وقد تساهم في زيادة الاستقطاب الديني والمذهبي وتعرقل أي مساعي للمصالحة.^{٤١}

- ارتبطت ظاهرة الاستقطاب السياسي في البحرين، بالمعلومات التي يتم تبادلها عبر وسائل الإعلام الاجتماعية، حيث تحولت تلك الوسائل لتبادل الهجمات الطائفية بين السنة والشيعة على نحو متزايد، وتحولت لغة الخطاب السياسي إلى خطاب طائفي يتضمن رسائل طائفية، عكست بوضوح الفجوة بين أنصار السنة والشيعة، وتفاعلت الجماهير مع هذا الخطاب بطرق عدائية.

ثالثاً: تهديد المصالح الأمنية والاستراتيجية:

يدرك المخططون الاستراتيجيون تماماً نقاط الضعف في الساحة الأمنية، وتشمل الاعتماد الكبير على أنظمة معقدة تعطل بسهولة، ووجود ثغرات أمنية تهدد قدرات في حفظ الأمن الداخلي ومنع الجريمة والدفاع ضد أي اعتداء خارجي^{٤٢}، ولذلك من أهم الحالات الواقعية التي استهدفت قدرات الدولة الدفاعية والأمنية مايلي :-

أ- محاولة اقتحام مواقع قاعدة سان انطونيو الجوية الأمريكية (تكساس) ٢٠٠٩.

ب- الهجوم الإلكتروني على منشآت إيران النووية في نوفمبر ٢٠٠٧، بهدف تخريب عملية تخصيب من خلال تغيير سرعة أجهزة الطرد المركزي، وقد أطلق الخبراء على الفيروس المستخدم (stuxnet 0.5).

ت- الهجوم الإلكتروني الشامل على دول أوروبا الشرقية ودول الاتحاد السوفيتي السابق في أكتوبر ٢٠١٢ وهو ما عرف بـ "أكتوبر الأحمر"، حيث تمكن القراصنة من خلال جمع المعلومات عن نقاط الضعف في برنامجي word - excel التابعين لشركة ميكروسوفت، وقام القراصنة بجمع المعلومات من السفارات الحكومية ومراكز الأبحاث وشركات الطاقة والبنية التحتية النووية والبنيات التحتية الأخرى لهذه الدول.

ث- الهجوم الإلكتروني المتكرر على حلف الناتو (NATO)، حيث تجاوزت الهجمات حد (٥٠٠)

هجوم.

ج- التجسس الإلكتروني الإسرائيلي على مفاوضات إيران النووية مع مجموعة الخمس من خلال فيروس " الديدان الإلكترونية " وهو ما يعرف باسم " دوكو ٢ " للتجسس على شبكات الفنادق التي استضافة المفاوضات.

ويمكن تلخيص مظاهر تهديد الاعلام الجديد للمصالح الأمنية والاستراتيجية للدول فيما يلي:

- أ- تنفيذ العمليات الارهابية داخل إقليم الدولة و ضد مصالحها بالخارج:
- تمارس الجهات الفاعلة المزيد من النفوذ في الفضاء الإلكتروني، وتشكل أكبر المخاطر الأمنية الوطنية في مجال الانترنت أكثر من المجالات الأخرى، بسبب انخفاض التكلفة النسبية لاستخدام أدوات هجوم متطورة واستغلال نقاط الضعف في أنظمة التشغيل والشبكات^{٤٣}، وضمان عنصر السرية، وامكانية التواصل مع قاعدة عريضة من الجمهور انخفاض التكلفة، التنقيب على المعلومات الاتصالات، التعبئة والتجنيد التخطيط والتنسيق، والحصول على التمويل^{٤٤}.
- طورت الجماعات الإرهابية البارزة التكتيكات والاستراتيجيات البعيدة المدى، وأصبحت أكثر مهارة في الاستفادة القصوى من تكنولوجيات الاتصال التي أصبحت في متناول يدها لتعميم العمل عبر منصات وسائل الاعلام الاجتماعية، مثل الفيسبوك، اليوتيوب، وتويتر^{٤٥}، مما يؤدي إلى زيادة الأنشطة الإجرامية داخل إقليمها^{٤٦}.
- تجنيد الأعضاء عبر الحدود الوطنية للدول، فعبر وسائل التواصل يمكن تحقيق ذلك فقط دون الاضطرار إلى السفر إلى الخارج والمخاطرة بكشف وكالات الاستخبارات للعنصر الارهابي، ومن ثم أصبح من السهل إنشاء خلية إرهابية افتراضية، اتسعت الرقعة الجغرافية أمام الجماعات الإرهابية والشركات التابعة، توفر فرص أفضل للتواصل مباشرة مع الأتباع، فالدور الذي تلعبه وسائل الاعلام الجديد هو أكثر ديناميكية عن الوسائل المستخدمة فيما قبل.
- نشر المعتقدات الايديولوجية، وجمع الأموال، ونشر المعلومات الخاطئة، وتبادل التكتيكات الإرهابية، وتأجيج الرأي العام ضد الدولة.
- الاتجاه المتزايد لاستخدام الإعلام الجديد كمنصة لتعليم صناعة العبوات الناسفة لشن الهجمات الإرهابية.

ح- التجسس على الدولة ومنشآتها ومواطنيها لجمع المعلومات عنها :

- استخدام أجهزة المخابرات الدولية وسائل الإعلام الجديد في تجنيد العملاء الجدد في الدول، واستغلال حالة عدم الاستقرار السياسي والأمني الذي تعيشه بعض الدول للتجسس وجمع المعلومات عنها.
- تشير الكثير من الأدلة والتقارير عن مراقبة إسرائيل لكافة التطورات في العالم العربي

وبخاصة لبنان، وقد أشارت دراسة إسرائيلية، أصدرها "معهد أبحاث الأمن القومي"، التابع لجامعة تل أبيب بعنوان: "لبنان: توجهات ورأي في مواقع التواصل الاجتماعي"، أن حوالي ١٠% من السكان الذين يستعملون شبكات التواصل الاجتماعي يميلون إلى قوى ١٤ آذار، وأن غالبيةهم هم من المذهب الاسلامي السني، وأن لبنان بات يجلس على برميل بارود يكاد ينفجر في اي لحظة، وأن الجدل داخل الشبكات الاجتماعية حول ضرورة نزع سلاح حزب الله، والمليشيات السنية والفصائل الفلسطينية يتعاضم، وأن اللبنانيين يعبرون عن شعورهم بأن الجيش عاجز عن نزع السلاح، لأن الأكثرية الساحقة من جنوده ينتمون إلى الطائفة الشيعية، وينحازون إلى الطائفة وليس للجيش... إلخ.^{٤٧}

- ولم يعد ضرورياً استخدام الأدوات التقليدية للسيطرة على الناس أو التحريض على الفتنة، فباستخدام الفيسبوك يمكن التسلسل للبنية الاجتماعية والسياسية في أي بلد.

- وقوع العديد من الأشخاص في فخ التجنيد كجواسيس دون أن يدركوا ذلك عن طريق تسجيل الدخول إلى غرفة دردشة والتحدث عن أي شيء، ثم يتم جمع وتحليل المعلومات واستخدامها في مرحلة لاحقة.

د- استهداف رجال الأمن الوطني والعسكريين:^{٤٨}

- لا يجب الاستخفاف والاستهانة بالمعلومات التي يبثها أفراد أسر العسكريين ورجال الشرطة عبر وسائل التواصل، لأنها قد تمثل مفتاح حل لغز بالنسبة للخصم المحتمل (سواء كان بالداخل أو الخارج)، بل هي جزء من اللغز، لأن وسائل الإعلام الجديد هي سيف ذو حدين: فهي تسمح بالوصول إلى معلومات استثنائية يمكن الوصول إليها عندما تنتشر للكلى وللمن يهمله الأمر، بما في ذلك الخصوم المحتملين الذين يمكنهم استغلالها لإلحاق الضرر.^{٤٩}

- نشر ضباط الأمن الوطني ورجال الشرطة المعلومات على مواقع الإعلام الاجتماعي يثير المخاوف الأمنية حول تعرض هؤلاء الذين نشروا تلك المعلومات الأمنية أو العسكرية للابتزاز أو الاختطاف، وهذه التصرفات تشير بلا شك إلى خطورة استخدام ضباط الأمن الوطني لوسائل الإعلام الاجتماعية، وتثير القلق من سهولة وصول العناصر الإجرامية والإرهابية لمثل تلك المعلومات التي يتم تسريبها سواء كان ذلك بقصد أو عن غير قصد.^{٥٠}

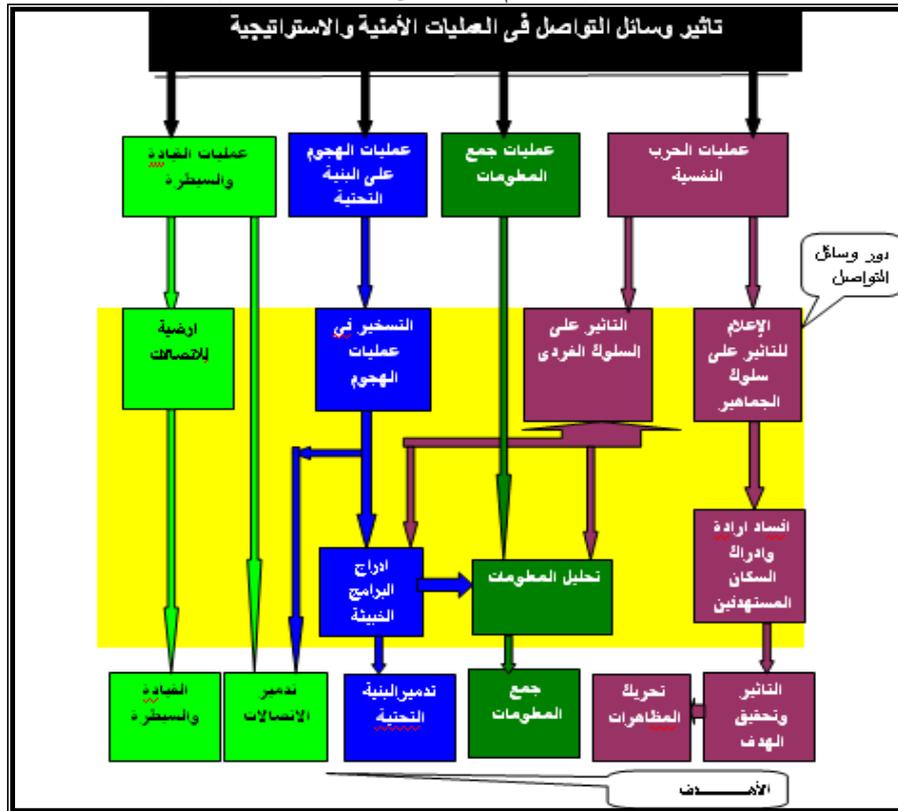
- تزايد قلق العديد من الدول من استخدام ضباط الأمن الوطني والعسكريين لوسائل الإعلام الجديد، وقد حذرت الهند في عام ٢٠١٢، جيشها من تهديدات وسائل الإعلام الاجتماعية للأمن القومي، عندما كشف أربعة من ضباط البحرية معلومات سرية عبر وسائل الإعلام الاجتماعية، وأيضاً أصدرت كوريا مبادئ توجيهية لجنودها، وقد حظر جهاز الأمن الاتحادي الروسي أعضائه من استخدام مواقع وسائل الإعلام الجديد بسبب بث معلومات عن مواقع عسكرية استراتيجية على الشبكات الاجتماعية الروسية، بما في ذلك معلومات عن الأسلحة النووية

والسفن الحربية الروسية.^{٥١}

- تتزايد التهديدات مع صعوبة الحفاظ على سرية تحركات رجال الشرطة والتحركات العسكرية في الداخل، بسبب أجهزة المحمول المجهزة بأحدث الكاميرات الرقمية المتكاملة وتطبيقات وسائل الإعلام الجديد، حيث يمكن قيام الشخص الذي لديه مثل هذا الجهاز بالتقاط الصور وتحميلها على منصة وسائل الاعلام، وربما يبث صور ومعلومات تحدد الموقع الجغرافي، ويوفر معلومة لأجهزة الاستخبارات الخارجية، لأن النقاط بيانات عن الوحدات العسكرية ومراكز التدريب الشرطة وتحديد الموقع الجغرافي يسمح للجماعات الإرهابية بمتابعة تحركات هذه الوحدات. وعلى اية حال، يوضح الشكل التالي دور الإنترنت وتقنيات الإعلام الجديد في العمليات الأمنية والاستراتيجية، عمليات الحرب النفسية، وعملية جمع المعلومات، وعمليات الهجوم على البنية التحتية، وعمليات القيادة والسيطرة، وفي الغالب تقوم هذه العمليات بدور مشترك ومتكامل، فقد تستهدف عملية الحرب النفسية الحصول على معلومات عن رد فعل الرأي العام عن سياسة يخطط لتنفيذها ببث شائعة كاذبة، وفي نفس الوقت فان الحصول على المعلومات وجمعها هو غاية مشتركة مع عمليات الاستخبارات وجمع المعلومات، وقد يكون الهدف من استخدام الإنترنت في عمليات الهجوم على البنية التحتية إدراج البرامج الخبيثة لتدمير بنية الاتصالات، وهو هدف عمليات القيادة والسيطرة، وهكذا تلعب هجمات الإنترنت دوراً محورياً ومتكاملاً في العمليات الأمنية والاستراتيجية.

شكل رقم (١)

تأثير الاعلام الجديد على المجالات الامنية والاستراتيجية



المصدر : من اعداد الباحث مستعينا على المرجع التالي :

المطلب الثاني

الإعلام الجديد والأمن الإقليمي في منطقة الخليج العربي

تشير الكثير من التقارير الى خسائر بمليارات الدولارات نتيجة القرصنة الالكترونية على مواقع المؤسسات المالية والشركات والبورصة، شركات الطيران، منشآت الطاقة والبتروك والغاز والكهرباء والصرف الصحي والطاقة النووية، وزارة الدفاع والأمن الوطني، القواعد العسكرية، وقد شهدت تلك المنشآت هجمات متكررة في دول عديدة، وأصبح هذا الصراع المعلوماتي والإلكتروني جزءاً من الصراع الدولي، بل يعتقد أن تلعب تكنولوجيا الإنترنت دوراً كبيراً في حروب المستقبل، وخاصة بين الدول المتقدمة، بل هي سلاح استراتيجي في يد الجماعات الإرهابية التي لاتستطيع المواجهة الشاملة مع القوى الكبرى مثل الولايات المتحدة، كما أن هذه الحرب الإلكترونية تدور بالفعل بين القوى الدولية، وهناك تنافس وسباق دولي بين القوى الكبرى لتحقيق أقصى استفادة من الإنترنت في تحقيق السيطرة والهيمنة على الفضاء الإلكتروني، فمن يسيطر على تكنولوجيا الإنترنت وهذا الكم الهائل من المعلومات يسيطر بلاشك على العالم، فالمعلومة والمعرفة التكنولوجية أصبحت مصدر من مصادر القوة الاستراتيجية للدول. لقد أثر التقدم التكنولوجي بالفعل على العلاقات الدولية وخاصة الصراعات الدولية، فهناك جانب كبير من العلاقات الدولية يدور عبر الفضاء الإلكتروني، فالحروب الإلكترونية بين الولايات المتحدة وكوريا الشمالية من اجل التشويش على الدعاية الأمريكية حول البرنامج النووي لكوريا الشمالية، والحروب الإلكترونية بين كوريا الشمالية وكوريا الجنوبية، الحروب الإلكترونية بين الصين والولايات المتحدة والصين وتايوان، الحرب الإلكترونية الروسية - الألمانية، الحروب الإلكترونية بين إسرائيل وحركة حماس في غزة، الحرب الإلكترونية بين إسرائيل وإيران حول البرنامج النووي الإيراني، التجسس الإلكتروني الأمريكي على دول العالم، والتجسس الإلكتروني الإسرائيلي على الدول العربية، والهجمات الإلكترونية للجماعات الارهابية على مصالح الدول، التجنيد والتمويل والتنسيق والتخطيط وتنفيذ العمليات الإرهابية.

ويمثل تطوير إيران لقدرات الهجوم الإلكتروني المصدر الرئيسي للتوتر في منطقة الخليج، إلى جانب القلق المتزايد حول قدرات الإنترنت الإسرائيلية، نظراً لأهمية منطقة الخليج الاستراتيجية والاقتصادية، فيمكن أن يؤدي استخدام أدوات الإنترنت الى تغيير ميزان القوى العسكري بين دول المنطقة وتقويض الاستقرار في الخليج، خاصة مع سعي إيران إلى تطوير قدراتها الإلكترونية، وهو ما تعتبره تهديداً أمنياً يفرض عليها ضرورة تنمية قدراتها الدفاعية، والتعاون مع حلفائها بشكل أكثر فعالية لردع التهديدات المستقبلية.

ويمكن تلخيص أهم تطورات الصراع الإلكتروني في منطقة الخليج على النحو التالي:^{٥٢}

- لقد كان الباعث على تطوير إيران لقدراتها في التقنيات الإلكترونية هو القلق من المعارضة، فخلال ٢٠٠٩ شهدت الكثير من الاحتجاجات الشعبية، فسعت قوات الأمن الإيرانية لمراقبة وتعطيل وصول حركات المعارضة إلى الإنترنت، بسبب الخوف من أن تؤدي الانتفاضة الشعبية

في إيران إلى الاطاحة بالنظام مثلما حدث في تونس ومصر في عام ٢٠١١. ومنذ ذلك الحين، قامت قوات الأمن الإيرانية بتوسيع قدراتها من رصد وعرقلة المعارضة على الانترنت إلى تحسين قدراتها على استخدام التقنيات الإلكترونية ضد الدول الأخرى.

- أنشأت إيران في عام ٢٠١١ "المجلس الأعلى للفضاء الإلكتروني" لتنسيق الجهود الأمنية في الهجوم والدفاع ، ويضم أعضاء من كبار المسؤولين في الأمن، وقد علق مسئولون بارزون علناً على قدرات إيران وأهمية الحرب الإلكترونية، مثل عبد الله أراغي نائب قائد الحرس الثوري الإيراني الذي قال : "لقد جهزنا أنفسنا بأدوات جديدة للحرب الإلكترونية في الفضاء الإلكتروني هو أكثر خطورة من الحرب المادية،".

- ساهمت الهجمات الاسرائيلية (فيروس ستكسنت) ضد المنشآت النووية الإيرانية في عام ٢٠١٠ في تغييرات كبيرة في السياسة الإيرانية، لكنها لم تكن فريدة من نوعها، فقد اكتشف الباحثون البرامج الخبيثة المستخدمة لأغراض التجسس أو الهجوم ضد دول الخليج العربي، فالهجمات التي تعرضت لها أرامكو السعودية في عام ٢٠١٢، نسبت إلى إيران، وهي بلاشك قد أضحت تهديداً لدول مجلس التعاون الخليجي، بشكل يحتم علي هذه الدول العمل مع الدول الصديقة لتحسين قدراتها الدفاعية، وخاصة ان هناك تقارير تفيد بتعاون روسي مع إيران وبتعاون ايران مع كوريا الشمالية في تطوير الهجمات الإلكترونية.^{٥٣}

- لقد أدى الهجوم إلكتروني إلى محو جميع البيانات على أجهزة الكمبيوتر في شركة أرامكو السعودية، وقد أصابت البرمجيات الخبيثة أنظمة العمل في المصفاة، وكشف حادث أرامكو عن التقدم من القدرات الإيرانية لإحداث أعمال تخريبية في دول الخليج، ناهيك عن سلسلة من الهجمات التي استهدفت وسائل الاعلام الخليجية، ونسبت إلى الجيش السوري الإلكتروني.

- هناك جهود متواصلة من قبل إسرائيل لاستخدام قدراتها الإلكترونية المتقدمة لأغراض التجسس الإلكتروني على العالم العربي وإيران.

- لا يبدو أن الصين قد لعبت دورا كبيرا في الخليج، لكن الدوافع الاقتصادية قد تغريها للتجسس على شركات الطاقة في الخليج لجمع المعلومات ذات القيمة التجارية. وبالتالي فان دول مجلس التعاون الخليجي بحاجة إلى تعزيز العلاقات وتوسيع الشراكات الأمنية القائمة على الأمن المعلوماتي. لأن الفشل في القيام بذلك سوف يزيد من مخاطر الهجمات الإلكترونية التي يمكن أن تؤدي إلى صراع إقليمي أوسع.^{٥٤}

والجدول التالي رقم (١) التهديدات الإلكترونية التي تستهدف القطاعين الحكومي والخاص في الدول العربية (٢٠١٥) ، يبين المؤشرات التالية^{٥٥} :-

- مصر والامارات والجزائر وليبيا وقطر من اكثر الدول العربية التي تتعرض للهجمات الالكترونية بفيروس " ستكسنت " على الإدارات الحيوية مثل الاتصالات، والبحوث

العسكرية والنفط. وتتعرض مصر لهجوم إلكتروني متكرر على منشآتها العسكرية، بينما تتعرض الجزائر أكثر لهجوم على منشآتها النفطية، وتتعرض الإمارات العربية المتحدة لهجوم على مراكز الأبحاث والدراسات.

- تتعرض المغرب والعراق والسودان والبحرين واليمن ولبنان والبحرين وسوريا بدرجة أقل للهجمات الالكترونية بفيروس " ستكسنت "، وتتعرض المغرب لهجوم أكثر على مؤسساتها الحكومية، بينما تتعرض السودان واليمن لهجوم أكثر على بنية الاتصالات، وتتعرض سوريا لهجوم إلكتروني متكرر على سفاراتها بالخارج.

وحاصل القول أن المنشآت النفطية في دول مجلس التعاون " الخليج العربي " هي أكثر القطاعات المعرضة للهجمات الالكترونية والتجسس الإلكتروني، حيث تستهدف القرصنة الالكترونية اما تعطيل عملية ضخ النفط، ومن ثم التأثير فيما بعد على اقتصاد هذه الدول أو التأثير على مستويات الأسعار، أو التجسس الاقتصادي، وقد يكون هذا الهجوم من جانب القوى المنافسة في السوق الدولي أو من جانب القوى المتضررة والتي تحاول أن تؤثر على مستويات الأسعار.

والأمر الأهم أن تطوير إيران ومساعدتها لتطوير قدراتها الإلكترونية وتحديثها المستمر لبنيتها التكنولوجية بالتعاون مع روسيا وكوريا الشمالية ودول أخرى، وكذلك تطوير إسرائيل أيضا لاستخدام هذه التقنيات يعني أننا أمام نوع جديد من الأسلحة الفتاكة قد يكون أقل تدميراً من السلاح النووي لكنه أسهل استخداماً وله تأثيره الاستراتيجي وتهديده الأمنى لمصالح الدول في الداخل والخارج. فالإنترنت أصبح سلاحاً استراتيجياً يصل إلى أهداف تعجز الأسلحة التقليدية عن الوصول إليها.

جدول (١)
التحديات الإلكترونية التي تستهدف القطاعين الحكومي والخاص في الدول العربية (٢٠١٥)

اخرى	السفارات بالخارج	الحكومية	بحثية	المالية	منشآت عسكرية	منشآت الطاقة	الاعلام	بنية الاتصالات	
++					++				مصر
			++				++		الامارات
++						++			الجزائر
++					++				ليبيا
++									قطر
	++	++							المغرب
++								++	السودان
++				++					العراق
++									البحرين
++	++								سوريا
++									لبنان
++								++	اليمن



المصدر : تقرير شركة كاسبرسكي kaspersky لعام ٢٠١٥

المبحث الثالث

استراتيجية الأمن القومي في عصر تكنولوجيا المعلومات

إن ما تواجهه الدول العربية من تهديدات قادمة من الفضاء المعلوماتي تحتم عليها ضرورة اتخاذ اجراءات سريعة ومتقدمة في مجال تطوير بنية الاتصالات والإنترنت والاستعانة بالخبرة الدولية في هذا المجال، ولاسيما في مجال الأمن المعلوماتي، وزيادة الإنفاق على البحوث والتطوير في مجال الهندسة الإلكترونية ودعم قدراتها الدفاعية في مواجهة الهجمات المتكررة بفيروسات الانترنت، غير أن مواجهة هذه التهديدات والتحديات لاينبغي أن يكون على الصعيد التكنولوجي فقط، إذ يمكن الاستفادة من الاعلام الجديد في الكثير من المجالات الأمنية والعسكرية والإعلامية، مثل في الاعلام الأمني والعسكري، إدارة الأزمات الأمنية الداخلية، مخاطبة الرأي العام الداخلي بشأن القضايا السياسية الداخلية، مخاطبة الرأي

العام الدولي بشأن السياسة الخارجية والشئون السياسية الدولية، ولذلك يجب على الدولة تعزيز قدراتها التكنولوجية، الأمنية، الدفاعية، الإعلامية.

المطلب الاول

استراتيجية الأمن القومي في عصر تكنولوجيا المعلومات

بلاشك إن وسائل التواصل الاجتماعي لها تداعيات خطيرة على الأمن القومي والمصالح الإستراتيجية للدولة، ومع ذلك، يمكن أن توفر فرص رائعة لتحقيق الأهداف الاستراتيجية ذات الصلة، ويمكن الاعتماد عليها في التنبؤ بتهديداتها والتصدي لها، فسوف يساعد ذلك في كيفية مواجهة آثارها السلبية، وبما أن وسائل الاعلام الاجتماعي تتطور بسرعة وتتفاعل مع العوامل الجغرافية والاقتصادية والاجتماعية والثقافية، فإن تطوير استراتيجية أمنية من خلالها يمكن أن يساعد في التعامل مع هذه التهديدات الجديدة. وفيما يلي يمكن عرض الاجراءات المقترحة لتعزيز قدرات الدولة في حماية الأمن القومي، على كافة الأصعدة التكنولوجية، والأمنية، والدفاعية والإعلامية:

أولاً: تعزيز القدرات الأمنية :

لم يعد من الممكن على أي دولة ان تعزل نفسها عن البيئة الرقمية المتغيرة، الأمر الذي يتطلب تكيف الأجهزة الأمنية في العالم العربي بطريقة مهنية واحترافية للاستفادة من الإمكانيات التكنولوجية الجديدة، لان الانعزالية تعنى التخلف والجهل بوسيلة ربما تكون مفيدة وخطيرة في نفس الوقت لما لها من تداعيات خطيرة ينبغى الوعي بها، لكن يمكن الاستفادة من ايجابياتها، فهذه الوسائل مصدر للبيانات والمعلومات ويمكن الاعتماد عليها في التصدي للجريمة في المجتمع ومكافحتها واتخاذ الخطوات الاستباقية لمنعها. وعلى سبيل المثال يمكن الاستفادة من تقنيات تكنولوجيا الإعلام الجديد في تعزيز القدرات الأمنية في الأغراض التالية:

١- دور الاعلام الجديد في إدارة الأزمة الأمنية:

بلاشك يضيف التطور التقني في تكنولوجيا الإعلام الجديد إمكانيات هائلة في مجال التعامل مع الأزمات الأمنية وإدارتها، خاصة عندما يستفحل الحدث الأمني ويتعدى فيه الوضع إلى الحد الذي يتطلب ضرورة تكاتف جهود العديد من الجهات الأمنية وغيرها، لمواجهة الاضرار المترتبة عليه بأقل جهد ووقت ممكن، وبأقل خسائر مادية وبشرية ممكنة، للحد من انتشار الأزمة ومنع تكرارها، خاصة إذا تطورت الأحداث بطريقة سريعة مما يؤدي إلى عدم الاستقرار والتوتر والاضطراب في الأمن.^{٥٦}

وتحتاج إدارة الأزمة الأمنية إلى مجموعة من الاستعدادات والجهود الإدارية التي تبذل للحد من الدمار المترتب على الأزمة لإنتاج استجابة استراتيجية للموقف الأمني، وإذا أردنا تطبيق ما سبق على إدارة الأزمة الأمنية في عصر تكنولوجيا الإعلام الجديد، فإننا نواجه تحدى تصاعد الأزمات الأمنية بسرعة غير مسبوقة^{٥٧}، حيث يمكن أن ينشر مروجى الشائعات خلال مراحل الأزمة المعلومات المغلوطة التي تنتقل بسرعة البرق عبر مواقع التواصل لتأجيج الرأي العام، مما يصعب من عملية

السيطرة على الأزمة في بداية مراحلها، ولذلك فإن استجابة الأجهزة الأمنية يجب أن تكون أسرع بالتصريح بالحقائق عن الأزمة عبر الصفحات الرسمية لها على مواقع التواصل أولاً بأول في مختلف مراحل تطورها، مروراً بالنشأة ثم الانفجار ثم الانحسار وما بعد الأزمة^{٥٨}، ويمكن من خلال وسائل الإعلام الجديد التقاط المؤشرات والتواصل مع الجمهور في كل مرحلة، بنشر المعلومة وتفسيرها، ويكون هذا الدور اخباري وتوجيهي، والتحدى هو صعوبة التحكم في نقل وتوجيه المعلومة عبر الشبكات، خاصة مع رصد انتهاكات وتجاوزات رجل الأمن مع الجمهور، حيث لا توجد فرصة متاحة لدى رجل الأمن مثلما كانت الفرصة في الاعلام التقليدي (حجب المعلومة).^{٥٩}

وعلى سبيل المثال، تكشف أزمة الانفلات الأمني في مصر عن أهمية دور الإعلام الأمني الذي يعتمد على وسائل التواصل الاجتماعي، ومن ثم أهمية دقة المعلومات للتأثير على الرأي العام والتعامل مع الجمهور، فقد نظر الجمهور إلى أزمة الانفلات الأمني على أنها أزمة مدبرة بفعل الشرطة، وتم استخدام وسائل التواصل في نشر اشربة الفيديو ونشر وثائق تشير الى خطة الأمن لإحداث انفلات أمني، مما أدى إلى تعميق حالة الانفصال وانعدام الثقة بين الشعب والشرطة، بينما ركزت جهود الشرطة المصرية في ادارة الأزمة الأمنية من خلال الإعلام الجديد على تبرير الممارسات الأمنية لاستخدام الغاز المسيل أثناء المظاهرات لتفريق المتظاهرين، وتفسير أزمة الانفلات الأمني بسقوط شهداء الشرطة والهجوم على السجون وأقسام الشرطة وحرقتها، ومن ثم نشرت صور ضحايا وشهداء الشرطة وصور لهروب السجناء، ومن ثم فقد كان اختلاط الآراء وارتباك المواقف نتيجة غياب المعلومة الدقيقة والموثقة مع عمومية توجيه الاتهامات، وفي ذلك دلالة هامة على أن السبيل الوحيد هو تقديم المعلومة الدقيقة الموثقة، فقد يتحول الاعلام الجديد الى آلية للتفتيت الاجتماعي في غياب معلومة موثقة مما يؤدي الى اختلاط الرأي في التفسير، في ظل أداء أمني ضعيف ومناخ ملائم للأزمة الأمنية.^{٦٠}

وفي الوقت الحالي تتركز الجهود الأمنية على استخدام وسائل الإعلام الجديد بدرجة أكبر كأداة للتواصل مع الجماهير، وقد بدأت بعض الأجهزة الأمنية بالفعل في مختلف دول العالم باستخدامها للإنترنت في جهود البحث والتحقيق للحصول على أدلة جنائية لكشف الجرائم وإلقاء القبض على المجرمين، ومثال ذلك، تمكنت الشرطة المصرية عن طريق تتبع حسابات العصابات الإجرامية على الفيسبوك وألقت القبض على العديد منهم، بل أنشأت العديد من وزارات الداخلية في العالم العربي مواقع لها على الفيسبوك للإعلان والإفصاح عن المعلومات للجمهور من أجل التوعية بالأعمال الإجرامية وتنفيذ الإشاعات والأكاذيب التي تبث عبر وسائل التواصل الاجتماعي وتهدد الأمن والاستقرار السلمي للمجتمع.^{٦١}

٢- دور الإعلام الجديد في الدفاع المدني :-

أظهرت الأزمات الأخيرة، أهمية الاعلام الجديد في جهود الإغاثة من الكوارث الطبيعية، حيث تسمح تكنولوجيا الاعلام الجديد بالتواصل بالمعلومات مباشرة، حيث تلعب وسائل الإعلام الجديد دوراً

هاماً ومساعدًا في تنسيق جهود الإغاثة للمدنيين، ويمكن الاستفادة منها في إدارة الأزمات وحالات الكوارث والطوارئ، ويمكن للوحدات الخاصة والعسكرية المشاركة في مثل هذه الأنشطة والاستفادة من السرعة التي توفرها منصات وسائل الإعلام الاجتماعية في إجراء الاتصالات والتنسيق بين العاملين العسكريين والمدنيين في جهود الإغاثة.^{٦٢}

ولذلك اهتم بعض الخبراء بتحديد استراتيجية شاملة لاستخدام ذلك النوع الجديد من الاعلام باعتباره وسيلة لفتح قنوات جديدة للتواصل والشفافية، فينبغي البدء بوضع مبادئ توجيهية لاستخدام وسائل الاعلام الجديد خلال الطوارئ، وينبغي توفير الموارد المطلوبة، والاستعداد لتلقى الانتقادات والرد بناء على تعليقات الجمهور، وينبغي على جميع مراكز عمليات الطوارئ أن تسعى جاهدة لنقل المعلومات الهامة، والمواد ذات الصلة مثل الصور أو أشرطة الفيديو من موقع الحادث بطريقة سريعة، فيمكن أن يكون الفيديو أو الرسالة الصوتية المرسلة مفيد في تهدئة الجمهور في حوادث الطوارئ، وأخيراً، ينبغي التنبيه بالمعلومات بشكل دوري ومتكرر أثناء الأزمة.^{٦٣}

ومن ثم فقد برز دور الإعلام الجديد في إدارة الأزمات والكوارث لعدة أسباب، أهمها، إنه يحقق مصداقية للمنظمة التي تعمل في جهود الإغاثة، ويسمح بالتخاطب والشفافية في الوقت الحقيقي واستقبال ردود الفعل من الناس حول الأزمة، وكانت منظمة الصليب الأحمر أول من بدأت استخدام وسائل الإعلام الجديد بعد إعصار كاترينا، حيث كان عليها أن تجد طريقة أفضل للتواصل مع أفراد المجتمع، وقد بدأت العمل بإنشاء غرفة أخبار عن الكارثة، وقد استطاع الصليب الأحمر القدرة على تصحيح المعلومات، والقدرة على جمع الأموال وحشد المتطوعين، وقد قام بتدريبهم في المدونات وتشجيعهم على نشر المعلومات خلال الأزمة، وليس ذلك سوى مثال من أمثلة عديدة من المنظمات التي تستخدم وسائل الإعلام الجديد للتواصل مع الجمهور خلال فترة الأزمات والكوارث.^{٦٤}

٣- دور الاعلام الجديد في البحث والتحقيق الجنائي :-

يستطيع رجال التحقيق الجنائي التعرف على الجناة والشهود وجمع المعلومات حول الجريمة ومركبيها وشهودها، وغيرها من المعلومات المتاحة حول الحادث من خلال وسائل التواصل الاجتماعي، والتي يمكن أن تستخدم كخيوط وأدلة في التحقيق الجنائي. ولكن يجب الإشارة هنا إلى أنه ثمة إشكالية أخرى هي؛ أن شهود الجريمة يمكن أن ينقلوا بسرعة المعلومات حول مسرح الجريمة أو الفعل الإجرامي إلى العالم عبر وسائل التواصل الاجتماعي، وإعاقة قدرة المباحث للسيطرة على المعلومات حول القضية، ومن ثم فإن التحدي الاستراتيجي لرصد الشبكات الاجتماعية وتحويل البيانات إلى معلومات يمكن أن يكون مهمة شاقة للشرطة، وينصح الخبراء جهات التحقيق عند استخدامهم تسجيلات الفيديو والصور للتحقيق في النشاط الإجرامي بالتعامل مع التدفق الكبير من المعلومات الواردة بحذر شديد، فيجب الحفاظ على مستوى معين من الشكوك حول هذه المعلومات، فقد يستبعد الفيديو الأحداث التي حدثت مباشرة قبل أو بعد الأحداث التي صورت في الفيديو، مما يؤدي إلى استنتاجات خاطئة، ويجب على جهاز الشرطة

أيضاً أن يكون في حالة تأهب ضد حملات القصاص ضد الأشخاص الذين يقومون بتسجيل الفيديو أو غيرها من المعلومات المنشورة على وسائل الإعلام الجديد عن الجريمة^{٦٥}، ويمكن لإدارات الشرطة استخدام وسائل الإعلام الاجتماعي للحصول على المعلومات، وخاصة لأغراض تكتيكية، مثل جمع المعلومات حول أعمال الشغب، أو النشاط الإجرامي، ودعوات الحشد للمظاهرات، التي تهتم الأجهزة الأمنية برصدها من أجل قياس مزاج الجماهير، وتقييم ما إذا كانت تمثل تهديدات إجرامية من عدمه، للشرطة في أعقاب أحداث الشغب.

ثانياً: الإصلاح التشريعي والتعاون الدولي للتصدي للجريمة الالكترونية:

وبما أن الحكومات الوطنية تهتم بإدارات الأمن ومكافحة الجريمة ضمن الأطر القانونية الوطنية، ووفقاً لقوانين حقوق النشر والملكية الفكرية، والسيطرة على الممارسات الضارة بمصالحها في الفضاء الإلكتروني، فإن الأمر يتطلب ضرورة إعادة النظر وإجراء بعض التعديلات التشريعية على القوانين واللوائح بشكل مستمر لمواجهة التغيير المستمر في التقنيات التكنولوجية في المجال الإلكتروني، ولا تزال جهود اتحاد الاتصالات الدولية لوضع معايير جديدة للفضاء الإلكتروني غير فعالة، وتعكس وجهات نظر بعض الحكومات حول السيادة والقواعد المرغوب فيها على الإنترنت^{٦٦}.

وقد دعا بعض المحللين إلى مفاوضات للحد من الأسلحة الإلكترونية، ولكن الاختلاف حول المعايير جعل من الصعب التفاوض حول مثل هذه المعاهدات، وقد تكون الجهود الرامية إلى تطوير درجة التعاون الدولي للحد من الجريمة الإلكترونية مماثلة للجهود الرامية إلى التصدي لممارسات القرصنة في حقبة سابقة، حيث وجدت العديد من الحكومات هناك حاجة إلى الاتفاق على ميثاق القرصنة (إعلان باريس في ١٨٥٦)، واليوم الحكومات لديها موقف مماثل تجاه الجريمة على الإنترنت، على الرغم من رفض روسيا والصين التوقيع على اتفاقية مجلس أوروبا بشأن الجريمة الالكترونية، ولكن المواقف قد تتغير مع مرور الوقت ومع تجاوز تكاليفها حدود المعقول، وعلى مدى العقد الماضي، أقرت الجمعية العامة للأمم المتحدة مجموعة من القرارات تدين النشاط الإجرامي وتحدد التدابير الدفاعية التي يمكن للحكومات أن تتخذها^{٦٧}.

وإذا كانت السياسات تركز على إجراء تغييرات في التشريعات والقواعد والأطر التنظيمية باعتبارها الوسيلة اللازمة لزيادة الأمن، فهذه الأدوات والحلول غالباً ما تثير القيود الخاصة بها: وأهمها، أنه يجب أن يكون مطوري البرمجيات مسؤولين عن مستوى الثغرات الأمنية في منتجاتهم، ويستتبع ذلك أنه يجب أن تكون الأطراف قادرة على تمكين شركات التأمين للقيام بدورها، وهذا بدوره يجعل شركات التأمين تعمل بجدية حول تحليل المخاطر وفعالية المنتجات الأمنية، ثانيهما، أن تركز الشركات داخليا على آليات إدارة المخاطر وخدمات الاستعانة بمصادر خارجية، ولكن تشكو شركات التأمين من نقص الوعي بالمخاطر الالكترونية، والسياسات التي تزيد من الكشف عن المخاطر وتساعد في تحفيز النمو في سوق التأمين الإلكتروني، بالإضافة إلى صعوبة تقييم أمن المؤمن وتحديد الأقساط على أساس المعايير

التقنية، بينما يعتبر التأمين جزءاً من حل طويل الأجل لتحسين أمن الشبكات، وسوف يتطلب سياسات كافية للمساعدة في تحقيق ذلك.^{٦٨}

ثالثاً: تعزيز القدرات التكنولوجية:

يجب أن تركز الاستراتيجيات الأمنية في الدول العربية على الاستثمار في أمن البرمجيات لبناء نظم أكثر أمناً، وينبغي أن تضع الحوافز لشركات صناعة البرمجيات الأمنية، والنظر في منح إعفاءات ضريبية للشركات التي تقوم بتطوير برامج أكثر أمناً، وينبغي أيضاً نشر الإخفاقات الأمنية لتعزيز وعي الشركات والمستهلكين، وهناك العديد من طرق الهندسة الإلكترونية التي يمكن أن تساعد في تخفيف مخاطر الإنترنت، وهو أمر ضروري لتحقيق الأمن الإلكتروني والحفاظ على سلامة الإنترنت، إذا تم تصميمها على نحو أفضل، فسيكون من الصعب استغلال تلك الثغرات، وينبغي أن تركز الاستراتيجية على العمل الجماعي والاستجابة الدولية للتهديدات الإلكترونية، والتعاون في مجال حل مشكلة أمن البرمجيات، وفهم المخاطر ذات الصلة، وعلى الحكومات أن تقوم بتحديد المتطلبات الأساسية لتقييم فعالية نظام المراقبة الأمنية الإلكترونية.^{٦٩}

وهناك مناهج جديدة يمكن استخدامها من قبل الحكومات مثل النهج الوقائي لمواجهة انتشار الممارسات الإلكترونية الخبيثة، وتحديد طرق منع انتشارها، وأهمها: أولاً: الزام السلطات لجميع الجهات العامة والخاصة بتقديم تقارير الزامية عن السلامة الإلكترونية لتمكين الحكومة من تنفيذ إجراءات الإنذار المبكر، والشفافية في الفضاء الإلكتروني، ثانياً: التدخل السريع لوقف انتشار البرمجيات الخبيثة، والحماية ضد الضرر وكلها لها علاقة مباشرة بأمن الإنترنت، ثالثاً: وضع إطار للعمل من أجل تنظيم التعاون بين الجهات الفاعلة الحكومية وغير الحكومية في مواجهة البرمجيات الخبيثة.^{٧٠}

وبالتالي سوف يساعد هذا النهج في تحديد واتخاذ التدابير الوقائية في الفضاء الإلكتروني، وقد يكون هذا النهج أكثر قدرة على دعم الجهات الفاعلة الدولية الحكومية وغير الحكومية لأنه يعزز الأمن القومي، ويوفر وسيلة أكثر فعالية للحد من النشاط الضار وانخراط الجهات الفاعلة في الحرب غير النظامية في الفضاء الإلكتروني، ويجب أن تشمل الاستراتيجية أفكاراً متكاملة وأساليب مختلفة، ففي كل صراعات الإنترنت غير النظامية، قد يكون لدى المتمردين القدرة على الاختباء في المجال الإلكتروني، وانتهاج استراتيجية الحرب غير النظامية ويكون لديها القدرة على الإفلات من العقاب، وإن فهم الحكومات لهذه الأساليب غير النظامية يساعدها على تحسين أمنها.^{٧١}

رابعاً: تعزيز القدرات الإعلامية:

إن تطوير "استراتيجية وطنية" بقدرات عالية، يتطلب اتباع أساليب فعالة لمواجهة دعاية الخصوم (مثل حملات الدعاية أو التضليل)، وتحسين أداء الوكالات والمؤسسات الحكومية، مثل تقاسم المعلومات بين المؤسسات بشكل أكبر وأسرع، فضلاً عن الاستفادة منها في صنع القرار، وتعزيز موقف الدولة

الجيوستراتيجي ومصادقيتها الدولية، ومن خلال تنفيذ استراتيجية الدمج المتكامل لاستخدام وسائل الاعلام الاجتماعية مع وسائل الإعلام الأخرى.^{٧٢}

وتشمل الاستراتيجيات الرامية إلى التصدي لتهديدات الإنترنت مراقبة وسائل الإعلام الاجتماعي للتصدي لمروجي الشائعات، والانفصاليين، والحفاظ على منافذ للحوار الاجتماعي.^{٧٣}

خامساً: تعزيز القدرات الدفاعية والعسكرية :

إن تطوير استراتيجية رشيدة في الفضاء الإلكتروني لتعزيز الأمن الوطني يطلب اتخاذ إجراءات سريعة للتصدي للحرب الإلكترونية، وأن تأخذ هذه الاجراءات شكلاً من أشكال الردع الاستراتيجي (يختلف بالطبع عن المفهوم الكلاسيكي للردع النووي)، والبحث عن حلول تقنية لدعم القدرات الدفاعية والهجومية، تساعد في دعم مرونة شبكات البنية التحتية، أما بالنسبة للتجسس الاقتصادي عبر الإنترنت، والذي يعتبر حالياً الأشد ضرراً، فمن المرجح أن يستمر بلا هوادة ما لم تكن هناك استجابات جديدة، خاصة أنه من الصعب توقيع اتفاقيات دولية لوقف التجسس.^{٧٤}

ويجب أن تركز الاستراتيجية على تعزيز القدرات الدفاعية والهجومية على حد سواء لمواجهة عمليات القوى المعادية، ومكافحة التجسس في الفضاء الإلكتروني، والتعاون بين وزارات ومؤسسات الأمن العام والصناعة والإعلام والاتصالات وأمن الدولة، ويجب أن تشمل استراتيجية الفضاء الإلكتروني تشكيل لجان للدفاع الإلكتروني لتمكين القيادة والسيطرة والاتصالات والكمبيوتر والعمليات الاستخباراتية والمراقبة والاستطلاع.^{٧٥}

ويجب أن تبحث وزارات الدفاع والداخلية والأمن الوطني عن إجراءات متناسقة حول استخدام الشبكات الاجتماعية، بدلاً من السياسات المتضاربة ، فتارة تشجع استخدامها، وتارة تحذر من مخاطرها، فيجب أن تنتشر التوصيات بشأن الاستخدام الجيد للشبكات الاجتماعية، وتحاول انشاء شبكات اجتماعية عسكرية كأداة سهلة للتواصل بين الضباط وأسرههم، وإن كان بعض المحللين يرون في الشبكات الاجتماعية العسكرية بعض الصعوبات مثل صعوبة الزام العديد من العائلات بالالتزام بها، لأنهم سوف يتصرفوا وفق شعورهم بأنهم مراقبون مما يضعهم تحت درجة من درجات الضغط النفسي عند استخدامها، وبالنسبة لأولئك الذين تركوا الخدمة سيكون من الصعب إن لم يكن مستحيلاً تحقيق تغطية جيدة لتصرفاتهم للتأكد من تنفيذهم التوجيهات الأمنية الجديدة لاستخدام الشبكات الاجتماعية.^{٧٦}

وبرغم تلك الصعوبات لا تزال بعض الدراسات توصي بإنشاء وحدات أمنية للعسكريين ورجال الأمن لحمايتهم من استهداف الجماعات الإجرامية والإرهابية، وقد رأينا كيف استهدفت هذه الجماعات رجال الشرطة من خلال استخدامهم وسائل التواصل الاجتماعي في مصر، لذلك يُقترح بناء وتطوير وجهة لشبكات اجتماعية عسكرية أو شرطية أمنة من خلال إحداث التغييرات المطلوبة على إعدادات الأمان ، وإخفاء المعلومات لحماية رجال الأمن وأسرههم، وحث الأجهزة الأمنية لجميع رجال الأمن وأسرههم

على استخدام هذه التطبيقات الموصى بها، وتحميلها وتثبيتها على أنظمة الكمبيوتر المنزلية والأجهزة النقالة، وترقيتها وتحديثها لمواجهة التهديدات الأمنية الجديدة.^{٧٧}

وعلى أية حال، فإن تقييم أهمية هذا المقترح يحتاج إلى دراسة من المتخصصين في مجال البرمجة وتكنولوجيا الإنترنت، وأن أى استراتيجية أمنية ينبغي أن تتضمن دراسة للقضايا المتعلقة بالشبكات الاجتماعية داخل المؤسسة العسكرية أو المؤسسات الأمنية، والقضايا المتعلقة بالمعلومات الأمنية وأفراد الأمن وأسرهم، ومشكلة تسرب هذه المعلومات، وعلى وجه الخصوص، تبادل المعلومات عن غير قصد والبيانات الوصفية المرتبطة بالشؤون العسكرية والشرطية، وتحتاج هذه المشاكل الأمنية من الدولة التدخل بشكل جديد ومحترف لحماية العسكريين وأسرهم، وهناك أيضاً حاجة لتطوير نظم وأبنية يمكن من خلالها التعامل مع البيانات الكبيرة وتحليلها داخل الفضاء الإلكتروني في الوقت الحقيقي، وهذا بلا شك يتطلب بناء نظم جديدة ومبتكرة يمكن تحليلها وتصنيفها بهدف تشكيل المعلومات المفيدة ووضع القواعد لاستخدامها مثل البيانات المتوفرة على الشبكات الاجتماعية اليوم.^{٧٨}

وإجمالاً، يمكن القول أن هناك مناهج مختلفة تستخدم لتحقيق الأمن الإلكتروني وهى: النهج الفني، والنهج الجنائي ونهج الحرب، ويعنى النهج الفني أن الفضاء الإلكتروني سيكون أكثر أمناً مع التقنيات الأمنية، وهذا النهج يتجسد فى هندسة البرمجيات، والاستجابة للحوادث بعد وقوعها، وتحليل الردود المحتملة للمهاجمين والبرمجيات الخبيثة، ويمكن أن تكون الحلول التقنية بمثابة الأساس ولكنها على الأرجح ليست كافية لمواجهة التحديات، ومن ثم يأتى دور النهج الجنائي فى رفع الدعاوى الجنائية أو المدنية ضد الجهات التى تعمل بشكل ضار فى الفضاء الإلكتروني، وقد يكون هذا نهجاً فعالاً، لكنه يتطلب تعديل التشريعات القائمة فى الدول العربية، لأن هناك خلافات فى القوانين حول العقوبات والإجراءات المحظورة، ونقص المدربين من رجال الشرطة والقضاة فى هذا المجال، ومشاكل الأدلة الجنائية الرقمية، والإجراءات الحكومية البطيئة، وبرغم أن هناك معايير قانونية على المستوى الدولي وتقاليد طويلة الأمد فى تعاون الدول للحد من الجريمة وتقديم المجرمين إلى العدالة لا تزال الجهود الدولية للتعاون فى هذا المجال غير مرضية، بينما نجد أنه يمكن من خلال نهج الحرب وتحسين القواعد والأنظمة العسكرية الإلكترونية القائمة^{٧٩}، وهذا يعنى أننا بحاجة إلى استراتيجية متكاملة على كافة الأصعدة تتعاون فيها مختلف الأجهزة الحكومية والوزارات، وتكثيف التعاون الدولي مع الحكومات والمؤسسات الدولية.

المطلب الثاني

مستقبل الأمن القومي في عصر تكنولوجيا المعلومات

إن نمو وتطور تكنولوجيا التواصل الاجتماعي في المستقبل يعتمد على قدرتنا على تطبيق سيادة القانون، واحترام الأعراف الاجتماعية المناسبة وأمن الفضاء الإلكتروني، ويتوقع البعض الحصول على شبكة إنترنت أقل تكلفة وأكثر سهولة في جميع أنحاء العالم، وسوف يكون الإنترنت، إذا لم يكن بالفعل، جزءاً من البنية التحتية العالمية، وفي المقابل ترى وجهة نظر أخرى أن انعدام الأمن الإلكتروني قد يتسبب في انخفاض قيمة الفضاء الإلكتروني، ومن ثم فإن تزايد العوامل التي تساعد على تطوير وتعزيز قيمته المتزايدة، سوف يضعف من احتمالات المخاوف الأمنية.^{٨٠}

إن التصدي للمخاطر الأمنية عبر وسائل التواصل الاجتماعي يتطلب التوعية ونشر الوعي بالأساليب الجديدة لاختراق البيئة المجتمعية، ولابد أن يدرك الجميع إن البيئة الرقمية المتغيرة وما تتيحه من إمكانيات متغيرة تعني إننا أصبحنا بحاجة إلى أن نفهم خصائصها حتى يمكننا تطويعها لصالح الأمن العام والقومي، وبالتالي يجب الاستخدام الحذر لهذه التقنيات، وإذا كان العلماء قد استطاعوا الاستفادة من الطاقة النووية في توليد الكهرباء والأغراض الصحية، على الرغم من أنها تستخدم كسلاح عسكري للفنك بالأعداء، فيمكن أيضاً الاستفادة من هذه الأداة الجديدة في الأغراض الأمنية، على الرغم من خطورتها الفتاكة بالمجتمع.

ويمكن القول أن هناك سيناريوهين لمستقبل الفضاء الإلكتروني على النحو التالي:^{٨١}

١- السيناريو المثالي: الانفتاح والأمن:

ومؤدى هذا السيناريو ان بيئة الإنترنت سوف تتجه تصاعدياً نحو الانفتاح والأمن؛ حيث تزايد قيمته في المجتمع محلياً وعالمياً بشكل متزايد، ويمكن إبراز خصائص هذا التطور، في حرية الوصول إلى الإنترنت واستخدام التطبيقات في مجال الصحة والتعليم وتطوير القدرات الدفاعية والأمنية، وتطوير سياسات أكثر تنسيقاً للحكومات الإقليمية ومؤسسات الإنترنت، محلياً ودولياً على حد سواء، واعتراف وتعاون الدول الكبرى بأهمية تأمين بنية الإنترنت، لأن البنية التحتية هي أداة تمكينية وأمر أساسي لنجاحها، ويصاحب ذلك تطور في الهندسة الإلكترونية للتصدي للتهديدات الأمنية، حيث يعتقد أن شركات مثل مايكروسوفت، وساب، وأدوبي قد قطعت شوطاً كبيراً في أمن البرمجيات لبناء برامج أكثر أمناً، بشكل يساعد على تحقيق الردع الأمني، وأيضاً للتصدي للجريمة الإلكترونية والتجسس الإلكتروني والحفاظ على السلام الإلكتروني، ومن ثم فإن تعزيز أمن البرمجيات وهندسة الأمن هو إلى حد كبير استجابة ناجحة لتهديدات الإنترنت.^{٨٢}

ويرى الخبراء أن التطور المستمر في تكنولوجيا التواصل سوف يمكن من تحقيق الأمن الإلكتروني بمستويات عالية من خلال تطوير بنية الكائن الرقمي بإنشاء فئات جديدة من الأجسام الرقمية، وهياكل للبيانات وتعليمات للتخزين وخصائص وسجلات معاملات تحتوي على بيانات وصفية،

والتي ستعمل أساساً كجدار عازل بين أوضاع الوصول والمحتويات، وبلا شك إن إعادة هندسة المعلومات والبنية التحتية سوف يقلل من التهديدات الأمنية، وتجدر الإشارة إلى أن هذا النموذج يحقق الوصول الآمن وحماية الملكية الرقمية، فضلاً عن الهياكل الرقمية التي يمكن أن تتطور على مر الزمن، ويمكن أن تؤدي إلى تنظيم البيانات التي تحقق كفاءة الوصول الآمن، كما أن تغيير المعايير الاجتماعية وتغيير ثقافة القرصنة وعدم الاعتراف بها سوف يجعل القرصنة سلوكاً غير مقبولاً اجتماعياً، ومن المهم أن نلاحظ أنه لن يكون هناك حرب إلكترونية أو إرهاب في السيناريو المثالي.

٢- السيناريو الأسوأ: الهجمات والصراع المستمر:

في مثل هذا السيناريو فإن هجمات قرصنة الكمبيوتر سوف تتزايد، وبالتالي تتلاشى القيمة الاقتصادية والاجتماعية للإنترنت؛ بشكل يؤثر على فعالية الفضاء الإلكتروني كأداة للمشاركة السياسية، والتعبير الثقافي، والتعليم والابتكار، بسبب ضعف القيادة العامة والخاصة، وسوء الإدارة المشتركة بين الحكومة والشركات في التعاون بشأن الفضاء الإلكتروني، مما يؤدي إلى انخفاض الكفاءة الأمنية، واستمرار تزايد التهديد المستمر بالصراعات الإلكترونية، ونظراً لانخفاض تكلفة الأسلحة الإلكترونية للغاية، يصبح السلاح الإلكتروني هو السلاح المفضل، فتتزايد الصراعات الإلكترونية داخل وفيما بين الدول، التي يمكن أن تظل في الفضاء الإلكتروني أو تمتد إلى الفضاء المادي بالهجوم على البنية التحتية، وبالتالي زيادة الإرهاب والجريمة الإلكترونية، حيث ينشط الجواسيس لسرقة المعلومات، ولا شك إن سرقة الممتلكات الفكرية، يؤدي إلى عدم كفاية الأمن الإلكتروني بالكامل، لوجود نظم أمن ضعيفة، ومن ثم تتزايد الاختراقات حيث تتزايد قدرة الهاكر *hacktivists* على تطوير أدوات جديدة، وبالتالي انعدام الأمن والتعدى على الخصوصية.

أنا سوف نواجه مجموعة من التحديات، ولن يكون التحول سلساً، وسيكلفنا أكثر إذا لم نتمكن من مواجهة هذه الأزمات بشكل فعال، ومن ناحية أخرى، فإننا قد نتحرك نحو دائرة السيناريو الأسوأ، إذا ضعفت السيطرة على الفضاء الإلكتروني وفشلنا في الاستجابة بفعالية لسلسلة من الأزمات، مثل الحروب الإلكترونية والإرهاب الإلكتروني التي تؤدي إلى تفتت البنية التحتية للمعلومات وتفتت الجريمة على الإنترنت، وبالتالي، هناك أيضاً اثنين من السيناريوهات التي تكمن بين هذين النقيضين: التحرك في الاتجاه الصحيح ولكن بشكل ناقص وليس على نحو سلس، أو التحرك في الاتجاه الخاطئ، ولكن أيضاً بشكل ناقص وليس على نحو سلس.^{٨٣}

ولكن بإمكاننا التقدم نحو السيناريو المثالي، ويتطلب تعزيز الجهود الحكومية للسيطرة وحوكمة الإنترنت، واعتماد قواعد ومعايير سلوك مشتركة وتشجيع على دعم البحوث التي تهتم بإعادة تصميم بنية الإنترنت لتقليل التهديدات الأمنية، والقيادة بسلاسة عبر الاستجابة الناجحة لمختلف أزمات الإنترنت، وسوف يساهم النمو الاقتصادي العالمي في زيادة منتجات وخدمات الإنترنت ذات الصلة، ومن المؤكد أننا سوف نواجه بعض أزمات الإنترنت في السنوات المقبلة، والسؤال الأساسي الهام هنا هو: ما إذا كانت

الحكومات العربية لديها الإرادة والقدرة على تحفيز وتنظيم الحوافز المناسبة للتحرك نحو السيناريو المثالي، وذلك لأن الإجراءات والخيارات السياسية أمام صناع القرار سوف تؤثر تأثيراً كبيراً على تطوير السياسة الأمنية في الفضاء الإلكتروني في المدى الطويل وسوف تؤثر على مستقبل أمن المجتمع.

خاتمة

مع تزايد التهديدات الأمنية القادمة من الفضاء الإلكتروني يتزايد اهتمام الأجهزة الأمنية بضرورة المواجهة والتصدي للجريمة الإلكترونية، التي تتزايد معدلاتها بشكل يفقد المواطنين الإيمان بسلطان الدولة، ولذلك تسعى الأجهزة الأمنية لمعالجة الجريمة والتعامل معها بمجموعة من الأساليب المتطورة، لتصبح وسائل الإعلام الاجتماعية ضمن دائرة اهتمام المراكز الأمنية والأجهزة الشرطة، ليس فقط في العالم العربي، ولكن في جميع الدول، وبالفعل أنشأت العديد من الأجهزة الشرطة لاسيما في العالم العربي صفحات لها على الفيسبوك للتفاعل مع المواطنين، للرد على الشائعات وتصحيح المفاهيم الخاطئة لدى الجمهور بهدف تحقيق الاستقرار السياسي، ولكن لا تزال هناك حاجة الى بذل الكثير من الجهود لحماية الأمن القومي من الحروب القادمة في الفضاء الإلكتروني.

أولاً : أهم نتائج الدراسة:

أ- هناك عوامل كثيرة تؤثر في مفهوم الأمن، بحيث إن أي تغير فيها يعنى التغير في مفهوم الأمن (مثل الثروة، الجغرافيا، القوة العسكرية، والبنية التحتية، القدرات الصناعية، والتعليمية، وهي في معظمها عوامل ملموسة، ويمكن قياسها بسهولة)، وعوامل أخرى مثل: (الاستراتيجية الوطنية، والقدرات التنظيمية والعلمية والفنية المعرفية، القدرات القيادية، والإرادة الوطنية والروح المعنوية، وهي عوامل غير ملموسة، وذاتية في المقام الأول، وأقل قابلية للقياس بسهولة)، والأهم من ذلك، الأهمية النسبية لعوامل الأمن القومي لدولة ما، فالمعادلة ليست ثابتة، لأنها تتغير بمرور الوقت، لأن الثورة التكنولوجية وتطور وسائل التواصل الاجتماعي وانتشارها قد غيرت بلا شك من طبيعة التهديدات الخارجية، مثلما أدت التطورات التكنولوجية العسكرية في الماضي إلى تراجع أهمية عنصر الجغرافيا في معادلة الأمن القومي للدول، مع ظهور حاملات الطائرات، والقاذفات النفاثة بعيدة المدى، والصواريخ العابرة للقارات، ومن ثم يتضح تأثير تطور تكنولوجيا وسائل التواصل الاجتماعي في مفهوم الأمن القومي، فقد أحدثت تغييراً في مجالات السيطرة، باعتبارها أداة أرخص وأسرع للتحرك في جميع أنحاء العالم بدرجة أسرع وبأقل تكلفة من تكاليف تطوير حاملات طائرات، والغواصات، تتلشى أمامها الحواجز بحيث يمكن للجهات الفاعلة غير الحكومية والصغيرة أن تلعب أدواراً هامة بتكاليف منخفضة نسبياً، وبحيث تكون جغرافيا الفضاء الإلكتروني هي أكثر قابلية للتغيير بكثير من البيئات الأخرى، فمن الصعب أن تتحرك الجبال والمحيطات، ولكن يمكن أن تتحول أجزاء الفضاء الإلكتروني بمجرد النقر على

مفتاح. وإذا كان لدى الحكومات احتكار واسع النطاق لاستخدام القوة في العالم الحقيقي، ولديها معرفة وثيقة بالتضاريس، وإنهاء الهجمات، لكن في العالم الافتراضي الجهات الفاعلة متنوعة، ومجهولة في بعض الأحيان، والمسافة المادية لا أهمية لها.

- ب- إن المعلومات التي يمكن أن تبث عبر وسائل التواصل الاجتماعي يمكن استخدامها كالتالي:-
- الحصول على مزايا استراتيجية في المجالات الأمنية والعسكرية، وخاصة على صعيد وضع الاستراتيجيات العسكرية والأمنية والاستخباراتية.
 - الحرب الإلكترونية، باعتبار أن الحرب الإلكترونية هي عبارة عن إجراءات تتخذها دولة ما لاختراق أجهزة الكمبيوتر أو الشبكات لدولة أخرى بهدف إلحاق الضرر باقتصادها أو بنيتها التحتية.
 - الإرهاب الإلكتروني: حيث يشار إلى الإرهاب الإلكتروني هنا بأنه استخدام شبكات التواصل الاجتماعي من قبل المنظمات الإرهابية للدعاية، أو لأغراض عمليات تهدد الأمن الوطني.
 - القرصنة الإلكترونية: حيث يشير مصطلح "القرصنة الإلكترونية" إلى الإجراءات المتخذة للهجوم على أجهزة الكمبيوتر.

ت- من أهم الآثار السلبية لتطور استخدام وسائل التواصل على الأمن، الحرب الإلكترونية والتجسس الإلكتروني، خطاب الكراهية والتحريض على العنف، الدعاية الكاذبة ونشر الشائعات والتضليل، إثارة السخط الشعبي، القرصنة في الفضاء الإلكتروني، والإرهاب الإلكتروني بشكل يثير الذعر، ويؤدي إلى الفوضى وعدم الاستقرار.

ث- من أهم الآثار الإيجابية، أن التطور التكنولوجي قد أضاف أبعاداً أخرى في مجال التعامل مع الأزمات الأمنية والدفاع الوطني وعمليات الإغاثة والطوارئ والتحقيق والتحريات وجمع المعلومات وقياس الرأي العام، فمع سرعة تصاعد الأزمات الأمنية بفعل نشر مروجي الشائعات خلال مراحل الأزمة المعومات المغلوطة التي تنتقل بسرعة البرق عبر مواقع التواصل لتأجيج الرأي العام، يمكن توزيع التحذيرات في حال حدوث حملات الدعاية والتضليل الكاذبة، وتثقيف المستخدمين حول التهديدات التي تشكلها وسائل الإعلام الاجتماعي، حيث لا تزال هذه الإجراءات من أفضل وسائل الدفاع في كشف التهديدات المحتملة.

ثانياً: أهم توصيات الدراسة:

تستطيع الحكومات الوطنية تحسين إجراءات الأمن القومي بكفاءة وفعالية بصياغة وتنفيذ استراتيجية مدروسة لضمان تحقيق الأمن الإلكتروني، وتطوير أدوات فعالة للتصدي للجرائم الإلكترونية، والتركيز على وضع القواعد التي يمكن تنفيذها على نحو فعال، ويمكن تلخيص أهم التوصيات الواجب الالتزام بها لوضع استراتيجية أمنية ملائمة على النحو الآتي :-

١- تعزيز حرية الإنترنت وتحقيق التوازن بين متطلبات حماية الخصوصية ومتطلبات الأمن القومي،

فيجب أن تتحرك الحكومات نحو تبني نهج متوازن في الفضاء الإلكتروني لا يجعل الخيارات صعبة بين الأمن والحرية، وبالتأكيد هناك صعوبة في تحقيق التوافق بين تأمين الفضاء الإلكتروني وتعزيز حرية الإنترنت، ولكن يمكن التغلب على ذلك بتحديد نطاق كل مفهوم، وفي هذا الصدد يجب أن نميز بين حرية الوصول إلى المعلومات، وحرية التعبير على الإنترنت، والحرية عبر الإنترنت في تعزيز حقوق الإنسان، والحريات المستندة إلى الإنترنت وأدوات التواصل، مثل الاحتجاج، والتنظيم، الخ، ومفهوم "الأمن الإلكتروني" الذي يعني حماية البيانات والأنظمة والشبكات التي ترتبط بالإنترنت، ومن ثم حماية الأمن القومي الذي يتطلب حماية الدولة ومواطنيها ومواردها وقيمها في الفضاء المادي والإلكتروني.

٢- يتعين على الدول العربية اتخاذ تدابير فعالة للتصدي للتأثير المدمر للإرهاب الإلكتروني، فقد يكون لمبادرات مكافحة الإرهاب المتعلقة باستخدام الإنترنت تأثير على التمتع بحقوق الإنسان، بما فيها الحق في حرية التعبير، والخصوصية والمحاكمة العادلة، لأن التحريض على الإرهاب قد ينطوي على فرض القيود على حرية التعبير، فحرية التعبير ليست حق مطلق، فيجب ألا تتجاوز اعتبارات حماية الأمن القومي، خاصة عند استغلالها للتحريض على التمييز أو العداوة أو العنف.

٣- هناك ضرورة لمنع وردع التحريض على الإرهاب لحماية الأمن القومي والنظام العام، وهذا يتفق مع الفقرة ٣ من المادة ١٩ من العهد الدولي الخاص بالحقوق المدنية والحقوق السياسية، وأيضاً وفقاً للفقرة ٢ من المادة ٢٠ من ذلك العهد، التي تخول الدول أن تحظر أي دعوة إلى القومية أو العنصرية أو الكراهية الدينية التي تشكل تحريضاً على التمييز أو العداوة أو العنف، في ضوء الطبيعة الأساسية للحق في حرية التعبير، ومن ثم يجب أن تكون القيود على ممارسة هذا الحق ضرورية ومتناسبة مع ما يشكله من تهديد.

٤- ينبغي حماية الأشخاص من أي تدخل تعسفي أو غير قانوني في الحق في الخصوصية، عندما تتضمن استراتيجية مكافحة الإرهاب المراقبة وجمع المعلومات المتعلقة بالمشتببه بهم، مثل جمع المعلومات حول هوية الفرد أو حياته خاصة، ويجب أن تكون القوانين المحلية مفصلة بما فيه الكفاية فيما يتعلق بجملة الأمور التي يجوز السماح فيها بهذا التدخل، ويجب أيضاً أن تكون الضمانات مناسبة لمنع إساءة استخدام أدوات المراقبة السرية، ويجب أن تضمن عدم الوصول غير القانوني أو التعسفي لجمع أي بيانات شخصية، وضمان الحق في تنفيذ إجراءات التقاضي السليم واحترام سيادة القانون عند اتخاذ تدابير فعالة لمكافحة الإرهاب، وحماية حقوق الأشخاص المتهمين بارتكاب جرائم جنائية، مثل الحق في البراءة، وتوفير الضمانات الواجبة خلال فترة زمنية معقولة أمام محكمة مستقلة ومحايطة ومختصة.

٥- يجب على وزارات الداخلية وقطاعات الأمن الداخلي في العالم العربي التعاون مع وزارات

- التجارة، وزارة الدفاع، وزارة العدل في تنفيذ الاستراتيجية الأمنية، وإشراك القطاع الخاص، ووضع معايير لسلوك المستخدم والسلامة الإلكترونية على الإنترنت والالتزام بتطبيق هذه المعايير.
- ٦- يجب إتباع مفهوم " الدفاع الإلكتروني الوطني المتقدم والمستمر "، ويجب على وزارة الأمن الوطني قيادة هذا الجهد، بدعم من وزارة الدفاع، وزارة الخارجية، ووزارة العدل بتشجيع هذا المفهوم للتعرف بشكل استباقي على الهجمات الخبيثة وإزالتها وتصفيتها.
- ٧- يجب أن تتعاون وزارات الدفاع مع وزارة الأمن الوطني في تحليل ديناميات "الحرب الإلكترونية غير النظامية" باعتبارها جانباً رئيسياً في عقيدة الحرب الإلكترونية، وينبغي أن تستمر وزارة العدل، وزارة الدفاع في متابعة مكافحة الإرهاب، ومكافحة التجسس، ويجب الاستمرار في تحسين والتكيف مع هذه الأساليب لمعالجة القضايا الإلكترونية.
- ٨- إنشاء جهاز مستقل، لتنفيذ استراتيجية الأمن الإلكتروني من أجل محاربة الإرهاب بطريقة فعالة.
- ٩- وضع القوانين المناسبة على المستوى الوطني والمحلي والدولي، وينبغي أن تتعامل القواعد والقوانين الرسمية على أنها أدوات تكميلية، فالإمكانيات التقنية وتمويلها هي مفتاح أي استراتيجية أمنية في الفضاء الإلكتروني.
- ١٠- التعاون العربي والدولي لمكافحة الإرهاب الإلكتروني وتنسيق الجهود الدولية والتفاوض على وضع معاهدة ملزمة حول مكافحة الجريمة عبر الإنترنت تلائم القضايا الأمنية المتغيرة مع التطور المستمر في تقنيات الإنترنت والتي تتطلب التدخل السريع. ويجب التشاور والتنسيق من خلال المنظمات الدولية المعنية حول وضع معايير دولية متفق عليها لتحقيق الأمن الجماعي وبذل الجهود الدولية الساعية إلى تحقيق التوافق والاتفاق على مبادئ وقواعد حرية الإنترنت والأمن الإلكتروني والإجراءات القانونية الواجبة، وهذا سوف يتطلب بلا شك تخصيص المزيد من الأموال أكثر من أي وقت مضى لتأمين الفضاء الإلكتروني.
- ١١- البحث في أفضل أساليب التعامل مع ثغرات الهندسة الاجتماعية التي تساعد في اتخاذ الإجراءات اللازمة للتصدي للهجمات وحماية الأنظمة التي هي جزء من شبكة الإنترنت، لإن الهندسة الاجتماعية تؤثر على طبيعة الأنشطة على الإنترنت، وبالتالي يحتمل أن تكون أكثر تحدياً ضد الهجمات الإلكترونية، ومن شأنها أن تساعد في تنفيذ استراتيجيات فعالة على الإنترنت.

الهوامش:

- ¹ Brett Van Niekerk and Manoj Maharaj : "Social Media and Information Conflict", **International Journal of Communication**, (Los Angeles: USC Annenberg School for Communication & Journalism, vol. 7, 2013), pp.1162–11645
- ² Capt. Cc Alfonso Montagnese : "Impact of Social Media on National Security ,Centro Militare Di Studi Strategic, **Research Paper**, (Rome (Italy): Stituto Alti Studi Per La Difesa (I.A.S.D.),and Istituto Superiore Di Stato Maggiore Interforze(I.S.S.M.I.) Stepi - Ae-U-3, February 2012)., pp.2-7.
- ³ Ambady, N., Hallahan, M., & Rosenthal, R: "On Judging and Being Judged Accurately in Zero-Acquaintance Situations", **Journal of Personality and Social Psychology**, (Washington, DC: American Psychological Association ,1995), p. 69
- ⁴ Julia Heidemann, Mathias Klier, Florian Probst: " Online Social Networks :A Survey of a Global Phenomenon", **Discussion Paper**, (Augsburg, Germany: University of Augsburg, Research Center Finance & Information Management, Department of Information Systems ,Engineering & Financial Management,2012),pp.1-10
- ⁵ Sumeet Gupta and Hee-Woong Kim : "Virtual Community : Concepts, Implications, and Future Research Directions ", **Proceedings of the Tenth Americas Conference on Information Systems**, New York, August 2004, pp. 2679-1686
- ⁶ Boyd, D. M., and Ellison, N. B. : "Social Network Sites: Definition, History, and Scholarship", **Journal of Computer-Mediated Communication**, (Hoboken, New Jersey: Wiley-Blackwell, 13(1) (2007), pp.210-220
- ⁷ Suomen Toivo -Think Tank : "Social Media - The New Power of Political Influence", **Version 1.0 Ari-Matti Auvinen**, (Brussels : Centre for European Studies ,2013), pp.10-20
- ⁸ Daniel S. Papp and David S. Alberts : "National Security in the Information Age: Setting the Stage, in , David S. Alberts and Daniel S. Papp (eds): **Information Age Anthology: National Security Implications of The Information Age**, (Washington, DC: Library of Congress Cataloging-in-Publication Data, Volume II of Information Age Anthology: National Security Implications of the Information Age, August 2000), pp.1-10
- ⁹ **Ibid** , p.10-23
- ¹⁰ **Ideam**
- ¹¹ سعد بن عبيد السبيعي : الإعلام الجديد ودوره في تعزيز الأمن الوطني في المملكة العربية السعودية ، دراسة تطبيقية على بعض النخب السعودية في مدينة الرياض، رسالة دكتوراة، (الرياض : جامعة نايف العربية للعلوم الأمنية ، ٢٠١٣)، ص ٩٨
- ¹² Martin C. Libicki : " Seven Types of Information Warfare", in , David S. Alberts and Daniel S. Papp (eds), **op.cit**, pp.77-99
- ¹³ Capt. Cc Alfonso Montagnese , **op.cit**, pp.3-7
- ¹⁴ د. فيليب تايلور ، سامي خشبة (مترجم): **قصف العقول : الدعاية للحرب منذ العالم القديم حتى العصر النووي**، سلسلة عالم المعرفة، (الكويت : المجلس الوطني للثقافة والفنون ، ٢٠٠٠)، ص. ٢٣
- ¹⁵ Joseph S. Nye, Jr.: Power and National Security in Cyberspace, in ,Kristin M. Lord and Travis Sharp (ed) : **America's Cyber Future : Security and Prosperity in the Information Age, Volume.II** ,(Washington ,D.C:Center for A New American Security , June 2011),pp.5-9
- ¹⁶ Daniel S. Papp and David S. Alberts ,**op.cit**,pp. 20-29
- ¹⁷ Capt. Cc Alfonso Montagnese , **op.cit**,pp.7.8
- ¹⁸ د. حميدة سميسم : **الحرب النفسية**، (بغداد : الدار الثقافية للنشر ، ٢٠٠٤)، ص ٣٠
- ¹⁹ Joseph S. Nye, Jr.,**op.cit**, p.10-13
- ²⁰ Martin C. Libicki, **op.cit**,pp. 94-99
- ²¹ Thomas G. Mahnke : "Cyberwar and Cyber Warfare", in ,Lord ,Kristin M. and Sharp ,Travis (ed) :**America's Cyber Future : Security and Prosperity in the Information Age, volume II** , Center for a new American Security , June 2011, p.61
- ²² Joseph S. Nye, Jr.,**op.cit**, pp.60-63
- ²³ Lior Tabansky : Cyber Crime: A National Security Issue?" ,**Military and Strategic Affairs**, The Institute for National Security Studies, Vol. 4, No. 3, December 2012, pp., p. 126.

²⁴ Majeed Khader: " Psychological Considerations for Digital Maturity:What are the Security Challenges and Implications?", **Report on The Workshop, " Social Media And Digital Maturity: Implications For National Security"** ,(Singapore :Nanyang Technological University ,The S. Rajaratnam School of International Studies (RSIS) ,The Centre of Excellence For National Security (CENS) , 31 October – 1 November 2013),p.5

²⁵ Lior Tabansky , **op.cit**,pp.121-123

²⁶ **Ibid**,123

²⁷ Joseph S. Nye, Jr: , **op.cit**,p.13

²⁸ Christopher M. Schroeder: " The Unprecedented Economic Risks of Network Insecurity", in, Kristin M. Lord and Travis Sharp (ed),**op.cit**, pp.165-170

²⁹ **Ibid**,pp. 170-171

³⁰ أحمد عبد العزيز الأصفر : " العوامل النفسية والاجتماعية لانتشار الشائعات وكيفية الوقاية من مخاطرها"، في أعمال ندوة **مواجهة الشائعات ، المنعقدة خلال لفترة ١٣-١٤/٤/٢٠١٠ بجامعة جيبوتي** ، ٢٠١٠، (الرياض : جامعة نايف للعلوم الأمنية ، لعدد ٣٥٦ ، ١٤٣٣ هـ)، ص ٧٧

³¹ مروة البشير: "الوعي الثقافي والديني أفضل السبل لمحاربة الشائعات" ، **الأهرام اليومي** ، ٢٠١٣/١/٤

³² د.ثامر كامل محمد : العولمة من منظور ثورة المعلومات وتكنولوجيا الاتصال وآليات حراكها في الوطن العربي ، **مجلة العلوم السياسية** : عدد خاص بالذكرى الخمسين لتدريس العلوم السياسية في العراق ،(بغداد : جامعة بغداد ، العدد (٣٧)،٢٠٠٨)، ص ٢٣٤

³³ Lior Tabansky , **op.cit**,pp.,p.121

³⁴ كوثر عباس الربيعي : الولايات المتحدة الامريكية والمراهنة على على الانترنت (مجدعات الطموح الامريكي للهيمنة في عصر المعلوماتية)، **مجلة المستقبل العربي**،(بيروت: مركز دراسات الوحدة العربية ، العدد (٣٨٧) ، ٢٠١١) .ص ص ٥٥- ٦٣

³⁵ Gregory J. Rattray and Jason Healey: " Non-State Actors and Cyber Conflict", in , Kristin M. Lord and Travis Sharp (ed) : **op.cit** ,pp.67-70

³⁶ مصطفى عصام نعوس : سيادة الدولة في الفضاء الالكتروني ، **مجلة الشريعة والقانون** ، (العين : جامعة الامارات العربية المتحدة ، كلية القانون ، السنة ٢٦ ، العدد ٥١ ، يوليو ٢٠١٢) ، ص ص ١٢٣-١٥٠

³⁷ Rob Schroeder, Sean Everton, and Russell Shepherd : "Mining Twitter Data from the Arab Spring, **CTX Vol. 2 No. 4** ,Special Issue :Social Media in Jihad and Counterterrorism ,Vol. 2, No. 4 ,<https://globalecco.org/mining-twitter-data-from-the-arab-spring>

³⁸ انظر بالتفصيل:

وليد رشا دزكي : المجتمع الافتراضي - نحو مقاربة للمفهوم " **مجلة الديمقراطية**، القاهرة ، مركز الأهرام للدراسات الإستراتيجية ، إبريل ٢٠٠٩ .

³⁹ د. فيليب تابلور ، سامي خشبة (مترجم)، **مرجع سبق ذكره**، ص. ٢٣

⁴⁰ أحمد عبد العزيز الأصفر ، **مرجع سبق ذكره**، ص ٧٧

⁴¹ راجع صحيفة البلد : " دراسة بريطانية: التواصل الاجتماعي في مصر ساحة للشائعات والتحريض.. ومرسي والبرادعي وشفيق فشلوا في استخدام "فيسبوك وتويتر" ، ٢٠١٣/١٢/٩

⁴² Brett Van Niekerk Manoj Maharaj , **op.cit**,pp. 1170–1174

⁴³ Gregory J. Rattray and Jason Healey,**op.cit** ,pp.67-70

⁴⁴ د.إيمان عبدالرحيم السيد الشرقاوي: جدلية العلاقة بين الاعلام الجديد والممارسات الارهابية : دراسة تطبيقية على شبكات التواصل الاجتماعي ، ورقة بحثية مقدمة الى مؤتمر دور الاعلام العربي في التصدي لظاهرة الارهاب ، **مجلة الامن والحياة** ، (الرياض : جامعة نايف للعلوم الأمنية ، ١٦-١٨ ديسمبر ٢٠١٤) ، ص ص ١٦ – ١٨

⁴⁵ انظر:

[Andrew Prempeh : "Social Media in the Era of Terrorism ,April 28, 2013.](http://www.foreignpolicyjournal.com/2013/04/28/social-media-in-the-era-of-terrorism/)

<http://www.foreignpolicyjournal.com/2013/04/28/social-media-in-the-era-of-terrorism/>

⁴⁶ انظر:

Joseph Kunkle : "Social Media and the Homegrown Terrorist Threat" ,police shief,

http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=2692&issue_id=62012

⁴⁷ Rania Massoud : Internautes libanais, Israël vous suit... de près;
[http://www.lorientlejour.com/article/767751/Internautes libanais%2C Israel vous suit... de pres.html](http://www.lorientlejour.com/article/767751/Internautes-libanais%2C-Israel-vous-suit...-de-pres.html)

⁴⁸ **Ibid**, 1180–1184

⁴⁹ Debbie Garside and (others): "Secure Military Social Networking and Rapid Sense making in Domain Specific Concept Systems: Research Issues and Future Solutions", **Future Internet**,(Basel, Switzerland : Future Internet Editorial Office ,March 2012...,pp.254-260

⁵⁰ Brett Van Niekerk Manoj Maharaj , **op.cit**,pp. 1162–1169

⁵¹ **Ibid**,, pp. 1162–1183

⁵² James Andrew Lewis : Cyber security and Stability in the Gulf, the CSIS Middle East Program issues periodic policy papers,(washington dc: center for strategic and international studies CSIS, middle east program ,January 20149,pp2,3

⁵³ **Ibid** ,3,4

⁵⁴ **Ibid** ,4-6

⁵⁵ Net Safe.Me : Cyber Espionage in Middle East , <http://netsafe.me/category/cyber-security/>

^{٥٦} سليمان حميدى الحميدى : فاعلية الاتصالات في ادارة الازمات الامنية باجهزة وزارة الداخلية بالرياض ، رسالة ماجستير ،(الرياض : جامعة نايف للعلوم الامنية ، ٢٠١٣)، ص ص ٤٦ ، ٤٧ ،
^{٥٧} محمد محمد الالفى : دور اعلام مواقع التواصل الاجتماعى في ادارة الازمة الامنية، ورقة عمل ،(الرياض : جامعة نايف العربية للعلوم الامنية ،)ص ص ١ - ٨

⁵⁸ Brett Van Niekerk and Manoj Maharaj , **op.cit**,pp. 1162–1184

^{٥٩} د. مها عبد المجيد صلاح : "الاعلان الجديد وإدارة الازمة الامنية " ، ورقة علمية مقدمة فى الملتقى العلمى : الاعلام الامنى ودوره فى ادارة الازمات ، عمان ، ٢٧ يونيو ٢٠١٢ .ص ص ١١ - ١٨
^{٦٠} المرجع السابق ، ص ص ١١ - ١٨
^{٦١} انظر :

Catherine Meszaros and (others) :Implications of International Events on Homeland Security : A case Study of The Arab Spring , **White Paper** , Prepared For Department of Homeland Security Office of Science and Technology, Homeland Security Studies and Analysis Institute , June 2012.pp.8,9

⁶² Brett Van Niekerk Manoj Maharaj , **op.cit**,pp. 1171

⁶³ Sara Prentice and Ethan Huffman : " Social Media's New Role in Emergency Management Emergency Management and Robotics for Hazardous Environments",**Working Paper** ,Idaho National Laboratory ,March 2008.,pp.1-3

⁶⁴ **Ibid**,pp.2,3

⁶⁵ **Office of Community Oriented Policing Services** ,U.S. Department of Justice :Social Media and Tactical Considerations For Law Enforcement,(Washington, DC: Police Executive Research Forum,and U.S. Department of Justice Office of Community Oriented Policing Services, May 2013),p.53

⁶⁶ Joseph S. Nye, Jr, **op.cit**,p.229

⁶⁷ **Ideam**

⁶⁸ Christopher M. Schroeder ,**op.cit**,pp.170-197

⁶⁹ Gary McGraw and Nathaniel Fick , Separating Threat from the Hype: What Washington Needs to Know about Cyber Security", in in, Kristin M. Lord and Travis Sharp (ed),**op.cit** , pp. 49-52

⁷⁰ Gregory J. Rattray and Jason Healey, **op.cit**,pp.70-77

⁷¹ **Ibid**,p. 77

⁷² Capt. Cc Alfonso Montagnese, **op.cit**,,pp.,7-10

⁷³ Danielle Kriz: "National Strategies for Information Security and Industrial Performance", National Strategies for Information Security and Industrial Performance", IGCC Workshop Report on China and Cybersecurity: Political, Economic, and Strategic Dimensions,(San Diego:University of California, University of California April 2012), pp. 14,15

⁷⁴ Joseph S. Nye, Jr.: **op.cit**,pp.25-29

⁷⁵ Danielle Kriz, **op.cit** , pp. 14,15

⁷⁶ Debbie Garside and (others),**op.cit**,pp.254-260

⁷⁷ **Ibid**,pp.253-258

⁷⁸ **Ibid**,pp.260-262

⁷⁹ Joseph S. Nye, Jr, **op.cit**,pp.226- 229

⁸⁰ Peter Schwartz: "Scenarios for the Future of Cyber Security", in ; Kristin M. Lord and Travis Sharp (ed) , **op.cit** ,p.219

⁸¹ **Ibid**,pp.219-228

⁸² Gary McGraw and Nathaniel Fick, **op.cit**pp.50-53

⁸³ Peter Schwartz , **op.cit**,pp.227

The study concluded that terrorist groups take advantage of New Media to communicate with cyber-crime groups and to coordinate along with them fundraising activities carried out in part or completely on the Internet.

It concludes that counter propaganda is used by the military to counter new media threats. And that the best news management comes from the military since they have a range of options for communicating their standpoint.

The study recommends that arab world countries needs to develop a comprehensive strategy that identifies roles, responsibilities, and resources across the government in order to detect, defend and pre-empt new media threats.

Keywords : Cybersecurity ,Intelligence , national security, new media, terrorism.

New Media Phenomenon and Its Impact on National Security

Dr. Hamdy Bashir

Researcher in the Arab political affairs
Faculty of Economics and Political Science
Cairo University

Abstract

New Media has become a mass communication tools, characterized by a global diffusion and an ever-growing level of use, considering their handiness and flexibility, as well as their extreme cheapness. It has become a central part of all cultures. People in all cultures are spending more time on new media than ever before.

This study examines the relationship between new media use and national security. There is significant work needs to be done in understanding the relationship between new media and national security. While new media was found to be an effective way to deliver information to large numbers of people, particularly in the event of a crisis, it is unclear whether it is a reliable source for factual information.

The purpose of this study is to analyze new media and national security threats in arab world. Specific objectives were to examine: the threats of new media technology to national security; the use of new media by the military in preventing, limiting or removing threats to national security; and the national security and how new media makes it worse; the use of new media in terrorist radicalization; the use of new media as an investigative tool.

The study found that the military use new media for military operations, communicating process of operation, boost morale of soldiers, clarify on propaganda messages sent by enemies and dispelling rumors, for updating civilians on progress of military operation. It found that the military uses new media as Open-Source Intelligence (OSINT) to analyze new media threats.

It found that new media are used by terrorist organizations as tools for ideological radicalization, recruitment, communication and training of its members. It found that terrorist groups take advantage of new media to communicate with cyber-crime groups and to coordinate along with them fundraising activities carried out in part or completely on the Internet.

Copyright © EPRA 2015

All rights reserved.

None of the materials provided on this Journal or the web site may be used, reproduced or transmitted, in whole or in part, in any form or by any means, electronic or mechanical, including photocopying, recording or the use of any information storage and retrieval system, except as provided for in the Terms and Conditions of Use of Egyptian public Relations Association, without permission in writing from the publisher.

And all applicable terms and conditions and international laws with regard to the violation of the copyrights of the electronic or printed copy.

ISSN for the printed copy

(ISSN 2314-8721)

ISSN of the electronic version

(ISSN 2314-8723X)

To request such permission or for further enquires, please contact:

EPRA Publications

Egyptian Public Relations Association, Gizza, Egypt
Dokki, Ben Elsarayat -2 Ahmed Elzayat St.

Email: chairman@epra.org.eg - jpr@epra.org.eg

Web: www.epra.org.eg

Phone: (+2) 0114 -15 -14 -157 - (+2) 0114 -15 -14 -151 - (+2) 02-376-20 -818

- The publication fees of the manuscript for the Egyptians are: 850 L.E. and for the Expatriate Egyptians and the Foreigners are: 450 \$.
- If the referring committee refused and approved the disqualification of publishing the manuscript, an amount of 250 L.E. will be reimbursed for the Egyptian authors and 130 \$ for the Expatriate Egyptians and the Foreigners.
- The manuscript does not exceed 35 pages of A4 size. 20 L.E. will be paid for an extra page for the Egyptians and 5 \$ for Expatriate Egyptians and the Foreigners authors.
- A special 10 % discount of the publication fees will be offered to the Egyptians and the Foreign members of the Fellowship of the Egyptian Public Relations Association for any number of times during the year.
- Three copies of the journal and three Extracted pieces from the author's manuscript after the publication.
- The fees of publishing the scientific abstract of (Master's Degree) are: 250 L.E. for the Egyptians and 150 \$ for the Foreigners.
- The fees of publishing the scientific abstract of (Doctorate Degree) are: 350 L.E. for the Egyptians and 180 \$ for the Foreigners. As the abstract do not exceed 8 pages and a 10 % discount is offered to the members of the Egyptian Society of Public Relations. Three copies of the journal will be sent to the author's address.
- Publishing a book offer costs LE 700 for the Egyptians and 300 \$US for foreigners.
- Three copies of the journal are sent to the author of the book after the publication to his/her address. And a 10% discount is offered to the members of the Egyptian Society of Public Relations.
- For publishing offers of workshops organization and seminars, inside Egypt LE 600 and outside Egypt U.S. \$ 350 without a limit to the number of pages.
- The fees of the presentation of the International Conferences inside Egypt: 850 L.E. and outside Egypt: 450 \$ without a limitation of the number of pages.
- All the research results and opinions express the opinions of the authors of the presented research papers not the opinions of the Egyptian Association for Public Relations.
- Submissions will be sent to the chairman of the Journal.

Address:

Egyptian Public Relations Association,
 Arab Republic of Egypt, Gizza, El-Dokki, Bein El-Sarayot, 2 Ahmed El-zayat Street.
 And also to the Association email: jpr@epra.org.eg, or epra_cairo@yahoo.com,
dr_hatematef2000@yahoo.com, after paying the publishing fees and sending a copy of the receipt.

Journal of public relations research Middle East

It is a scientific journal that publishes specialized research papers in Public Relations, Mass Media and Communication after peer refereeing these papers by a number of specialized Professors.

The journal is affiliated to the Egyptian Public Relations Association, the first Egyptian specialized scientific association in public relations.

- The journal is accredited, Classified internationally for its printed and electronic version from the Academy of Scientific Research and Technology in Cairo And classified by the Committee of Scientific Promotion Specialization media - Supreme Council of Universities.
- This journal is published quarterly.
- The journal accepts publishing books, conferences, workshops and scientific Arab and international events.
- The journal publishes advertisements on scientific search engines, Arabic and foreign publishing houses according to the special conditions adhered to by the advertiser.
- It also publishes special research papers of the scientific promotion and for researchers who are about to defend master and Doctoral theses.
- The publication of academic theses that have been discussed, scientific books specialized in public relations and media and teaching staff members specialized scientific essays.

Publishing rules:

- It should be an original Manuscripts that has never been published.
- Arabic, English, French Manuscripts are accepted however a one page abstract in English should be submitted if the Manuscripts is written in Arabic.
- The submitted Manuscripts should be in the fields of public relations and integrated marketing communications.
- The submitted scientific Manuscripts are subject to refereeing unless they have been evaluated by scientific committees and boards at recognized authorities or they were part of an accepted academic thesis.
- The correct scientific bases of writing scientific research should be considered. It should be typed, in Simplified Arabic, 14 points font for the main text. The main and sub titles, in Bold letters. English Manuscripts should be written in Times New Roman.
- References are mentioned at the end of the Manuscripts in a sequential manner.
- References are monitored at the end of research, according to the methodology of scientific sequential manner and in accordance with the reference signal to the board in a way that APA Search of America.
- The author should present a printed copy and an electronic copy of his manuscript on a CD written in Word format with his/her CV.
- In case of accepting the publication of the manuscript in the journal, the author will be informed officially by a letter. But in case of refusing, the author will be informed officially by a letter and part of the research publication fees will be sent back to him soon.
- If the manuscript required simple modifications, the author should resent the manuscript with the new modifications during one week after the receipt the modification notes, and if the author is late, the manuscript will be delayed to the upcoming issue, but if there are thorough modifications in the manuscript, the author should send them after 15 days.



Journal of Public Relations Research Middle East
(JPRR.ME)

Scientific Refereed Journal

- Seventh issue - July / September 2015

Founder & Chairman

Dr. Hatem Saad

Chair of EPRA

Editor in Chief

Prof. Dr. Aly Agwa

Professor of Public Relations & former Dean of Faculty
of Mass Communication - Cairo University
Chairman of the Scientific Committee of EPRA

Editorial Manager

Prof. Dr. Mohamed Moawad

Media Professor at Ain Shams University & former Dean of
Faculty of Mass Communication - Sinai University
Chairman of the Consulting Committee of EPRA

Editorial Assistants

Prof. Dr. Rizk Abd Elmoaty

Professor of Public Relations
Misr International University

Dr. Sadek Rabeh (Algeria)

Associate Professor of mass communication
the dean of Media and Public Relations - Emirates College
of Technology - Abu Dhabi - United Arab Emirates

El-Sayed Abdel-Rahman Ali

Assistant Professor of Public Relations
Mass Communication Faculty – Sinai University

Address

Egyptian Public Relations Association

Arab Republic of Egypt
Giza - Dokki

Ben Elsarayat - 2 Ahmed Zayat Street

Mobile: +201141514157

Tel : +2237620818

www.epra.org.eg

jpr@epra.org.eg

Scientific Board **

JPRR.ME

Prof. Dr. Aly Agwa (Egypt)

Professor of Public Relations and former Dean of the Faculty of Mass Communication, Cairo University

Prof. Dr. Thomas A. Bauer

Professor of Mass Communication at the University of Vienna

Prof. Dr. Mona Al-Hadedy (Egypt)

Professor of radio and television – Faculty of Mass Communication, Cairo University

Prof. Dr. Yas Elbaity (Iraq)

Professor of Journalism at the University of Baghdad, Vice Dean of the Faculty of Media and Information
and Humanities, Ajman University of Science

Prof. Dr. Enshirah el SHAL (Egypt)

Professor of Media at the Faculty of Mass Communication, Cairo University (State Doctorate in Arts and
Humanities from France)

Prof. Dr. Hassan Mekawy (Egypt)

Professor of radio and television – Faculty of Mass Communication, Cairo University

Prof. Dr. Nesma Younes (Egypt)

Professor of Radio & Television at the Faculty of Mass Communication, Cairo University

Prof. Dr. Mohamed Moawad (Egypt)

Media professor at Ain Shams University & former Dean of Faculty of Mass Communication - Sinai
University

Prof. Dr. Samy Abd Elaziz (Egypt)

Professor of public relations and marketing communications for the former Dean of the Faculty of
Information, Cairo University

Prof. Dr. Abd Elrahman El Aned (KSA)

Professor of Media and Public Relations Department of the Faculty of Media Arts - King Saud University

Prof. Dr. Mahmoud Yousef (Egypt)

Professor of Public Relations - Faculty of Mass Communication, Cairo University

Prof. Dr. Samy Taya (Egypt)

Professor and Head of Public Relations Faculty of Mass Communication - Cairo University

Prof. Dr. Basyouni Hamada (Egypt)

Professor of media and public opinion, political - Faculty of Mass Communication, Cairo University

Prof. Dr. Sherif Darwesh Allaban (Egypt)

Professor of printing press at the Faculty of Mass Communication, Cairo University

Prof. Dr. Hassan Aly (Egypt)

Professor of Radio & Television and Head of Mass Communication Department – Faculty of
Arts - Mina University

Prof. Dr. Mahmoud Hassan Ismael (Egypt)

professor of Culture Media and Children at Ain Shams University

Prof. Dr. Hamdy Abo Alenen (Egypt)

Media professor and dean of the Faculty of Al-Ahsan and Mass Communication, Vice President of the
International University of Egypt

Prof. Dr. Othman Al Arabi (KSA)

Professor of Public Relations and the former head of the media department at the Faculty of Arts – King
Saud University

Prof. Dr. Abden Alsharif (Libya)

Media professor and dean of the College of Arts and Humanities at the University of Zaytuna – Libya

Prof. Dr. Waled Fathalha Barakat (Egypt)

Professor of Radio & Television at the Faculty of Mass Communication, Cairo University

Prof. Dr. Tahseen Mansour (Jordan)

Professor of Public Relations at the Faculty of Mass Communication, Yarmouk University

Prof. Dr. Mohamed Elbokhary (Syria)

Professor, Department of Public Relations and Publicity, School of Journalism, University of MF Uzbek
national Ulugbek Beck

Prof. Dr. Ali Kessaissia, (Algeria)

Professor, Faculty of Media Science & Communication, University of Algiers-3.

Prof. Dr. Redouane BoudJema, (Algeria)

Professor, Faculty of Media Science & Communication, University of Algiers-3.

** Names are arranged according to the date of obtaining the degree of a university professor.

Journal



of P R research

Middle East

Journal of Public Relations Research Middle East

Scientific refereed Journal - Published by Egyptian Public Relations Association – Eighth Issue – July /September 2015

Abstracts Researches in Arabic:

- **Prof. Dr. Yass Al-Bayati** - Ajman University of Science & Technology
The role of the Social media in shaping social awareness in relation to sport hooliganism and crime from the viewpoint of the university students 7
- **Associate Prof. Dr. Ridha Mahmood Methmani** - Bahrain University
Enterprise strategy and Communication strategy: What kind of link ? 9
- **Associate Prof. Dr. Zohair Abdul Latif Abed Abed** - Al-Aqsa University
The Impact of Zionist Propaganda on The Palestinian Public Opinion During 2014 Aggression on Gaza Descriptive Study 11
- **Dr. Ibrahim Hassan El-Morsi Mohammed** - Sinai University
Patterns of Sinai Public Exposure to the Social Networks and Its Relationship to Formation of Opinion toward Current Events 12
- **Dr. Hamdy Bashir** – Cairo University
New Media Phenomenon and Its Impact on National Security 13
- **Dr. Maha Mustafa Omer Abdalaziz** – Emirates College of Technology - Abu Dhabi
Initiatives to protect intellectual property rights in the electronic environment "Copyright model" 15
- **Mohammed Amin Abu ob** – Hassiba Ben Bouali University - Algeria
Citizen journalism: from receiving to producing media content 17

(ISSN 2314-8721)

Egyptian National Scientific & Technical
Information Network

(ENSTINET)

Copyright ©2015 EPRA

www.epra.org.eg